Deliverable 5.1

Trial scenario Definitions and Evaluation Methodology Specification

Editor:	Ricard Munné (Atos)
Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Contractual delivery date:	28 February 2015
Actual delivery date:	15 May 2015
Suggested readers:	Smart city service developers, application developers, public administrations, service providers, researchers
Version:	0.07
Total number of pages:	143
Keywords:	RERUM, Internet of Things, smart cities, applications, use-cases, smart transportation, home energy management, environmental monitoring, comfort quality, trial scenario definitions, evaluation methodology

Abstract

This report provides the plan for testing the RERUM architectural framework and its components with regard to the technical objectives and innovations of the project, which is planned at two levels – through in-lab experiments and field trials. It provides the evaluation methodology, the evaluation criteria, the evaluation process, requirements, metrics and target. The aim of the in-lab experiments is to assess both qualitatively and quantitatively the performance gains of the protocols and algorithms, as well as the individual system modules developed in work packages WP2-WP4 to identify potential issues for the real-world trial phase in the pilot cities. The field trials to be performed in the two pilot cities are based on the four Use Cases as defined in D2.1. The trials will be performed in two phases. During the first phase Heraklion will test UC-O1 and UC-I1, and Tarragona UC-O2 and UC-I2. In the second phase the cities will test the UCs not tested in the first phase. In between the two testing phases a trial cross reporting activity will be performed to exchange the results of the trials to improve the trials in the second phase based on the experience gained through the first phase and the issues detected.

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	WP5 – Application Development, Experiments and Trials
Number and title of task	T5.1 – Trial Scenarios and validation
Document title	Trial scenario Definitions and Evaluation Methodology Specification
Editor: Name, company	Ricard Munné, ATOS
Work-package leader: Name, company	Ricard Munné, ATOS
Estimation of person months (PMs) spent on the Deliverable	

Executive summary

This report provides the plan for validating the RERUM architectural framework and its components with regard to the technical objectives and innovations of the project, which is planned at two levels – through in-lab experiments and field trials. Section 2 describes the evaluation methodology, which is based on the ISO standards for software product quality (ISO/IEC14598) [1] and for specifying metrics for product quality in software engineering (ISO/IEC9126) [2]. Evaluation criteria are also described, together with the evaluation process, requirements, metrics and target. Four groups of evaluation criteria have been defined: authorization, efficiency, performance and security.

Section 3 provides the description of the in-lab experiments to assess both qualitatively and quantitatively the performance gains of the protocols and algorithms, as well as the individual system modules developed in work packages WP2-WP4 to identify potential issues for the real-world trial phase in the pilot cities. The description of the experiments includes the specific purpose, the KPIs to measure (defined in the evaluation criteria in section 2), the scenarios description for the experiments, the functional components involved, risks and time plan. The experiments are focused on measuring the impact of the implementation of ECC signatures in the RERUM devices, the efficiency and performance of the adaptive Compressive Sensing keys, the performance of self-monitoring mechanism of RERUM devices, to evaluate the efficiency of the lightweight spectrum sensing and spectrum assignment frameworks, the efficiency of Cognitive Radio based gateway, the performance and efficiency of Android-based RERUM devices, the network performance of 6LoWPAN Multicast networks and the performance of DTLS protocol.

Section 4 describes the field trials to be performed in the two pilot cities based on the four Use Cases defined in D2.1 [3]. The trials will be performed in two phases. During the first phase Heraklion will test UC-O1 and UC-I1, and Tarragona UC-O2 and UC-I2. In the second phase the cities will test the UCs not tested in the first phase. In between the two testing phases a cross-evaluation of the results of the trials will be performed to improve the trials in the second phase based on the experience gained through the first phase and issues detected. The description of the trials includes the purpose, the deployment of RERUM components, the requirements and cross-dependencies and the scheduling of the testing activities, the risks and the specific KPIs and performance metrics of the UCs.

Finally, Section 5 provides a checklist of RERUM technical contributions that will be tested in the lab experiments and trials.

List of authors

Company	Author	Contribution
ATOS	Rodrigo Diaz	Initial ToC
	Ricard Munné	Reviewed ToC according meeting in Passau GA Evaluation methodology and Criteria definition template
	Dario Ruiz	Authorization criteria
	Cristo Reyes	Authorization criteria
UNIVBRIS	George Oikonomou	Performance Criteria Laboratory experiments
	Marcin Wójcik	Laboratory experiments
LiU	Vangelis Angelakis	Evaluation Criteria Proof-of-Concept Laboratory experiments Contribution to Trials
	David Gundlegård	Performance Criteria Proof-of-Concept Laboratory experiments
	Niklas Danielsson	Efficiency Criteria Proof-of-Concept Laboratory experiments
	Scott Fowler	Performance Criteria
UNI PASSAU	Henrich C. Pöhls	Laboratory experiments descriptions for On-Device Signatures (Section 3.1-3.4) and related KPI (AL.EF.3-5, AL.PE.3); Trials end users survey collaboration (Section 4.4)
ZOLERTIA	Antonio Liñán Marc Fàbregas	Tarragona Trials location and requirements Performance Criteria
FORTH	Alexandros Fragkiadakis Elias Tragos	Contribution to the Lab experiments, the evaluation criteria and the Heraklion trials. Reviewing the document.
CYTA	Athanasios Lioumpas	Heraklion Trials
AJTGNA	Xavier Reina	Tarragona Trials
HER	Manolis Fotakis	Contribution to the Heraklion trials definition.

	Costis Mochianakis	

Table of Contents

List of figures

List of tables

Abbreviations

3G	Third generation of mobile telecommunications technology
4G	Fourth generation of mobile telecommunications technology
6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
ABAC	Attribute-Based Access Control
AC	Alternating Current
A/C	Air Conditioner
ATC	Automatic Traffic Counter
API	Application Programming Interface
BMFA	Bi-Directional Multicast Forwarding Algorithm
CO	Carbon monoxide
CO2	Carbon dioxide
CoAP	Constrained Application Protocol
CPU	Central Processing Unit
CR	Cognitive Radio
CS	Compressed Sensing
DTLS	Datagram Transport Layer Security
DoS	Denial-of-Service
EC	European Commission
ECC	Elliptic curve cryptography
EM	Electro Magnetic
EMF	Electro Magnetic Field
GPRS	General Packet Radio Service
GVO	Generic Virtual RERUM Object
GW	Gateway
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
JSS	JSON sensor signatures
KPI	Key Performance Indicator
LAN	Local Area Network
MAC	Medium Access Control
MIME	Multi-Purpose Internet Mail Extensions
MPL	Multicast Protocol for Low power and Lossy Networks
MSE	Mean square error
MW	Middle Ware
mWh	micro Watt hour
NO2	Nitrogen dioxide
NOx	Mono-nitrogen oxides (nitric oxide and nitrogen dioxide)
O3	Ozone

OAP	Over the Air Programming
PC	Personal Computer
PCI	Peripheral Component Interconnect
PHP	PHP: Hypertext Preprocessor
PKI	Public Key Infrastructure
PM10	Particulate Matter 10 micrometer
PM2.5	Particulate Matter 2.5 micrometer
POST	HTTP POST request method
PRRS	Platform for Real time Reconfiguration of Security
QoS	Quality of Service
RAM	Random Access Memory
RD	RERUM Device
REST	Representational Transfer State
RH	Relative Humidity
ROM	Read Only Memory
RPL	IPv6 Routing Protocol for Low Power and Lossy Networks
RRD	Round-robin Database
RSS	Rich Site Summary
RSSI	Received Signal Strength Indicator
RTT	Round-Trip-Time
SA	Security Association
SDK	Software Development Kit
SDR	Software Defined Radio
SHA 256	Secure Hash Algorithm with 32-bit words
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
SO2	Sulfur dioxide
UC	Use-case
UDP	User Datagram Protocol
VOC	Volatile Organic Compounds
VPN	Virtual Private Network
VRD	Virtual Rerum Device
WAN	Wide Area Network
WiFi	Wireless local area network
XACML	eXtensible Access Control Markup Language
xDSL	Digital Subscriber Line
XML	Extensible Markup Language

1 Introduction

1.1 Objectives of this Document

The main objective of this document is to provide the framework for assessing the RERUM innovations, the definition of the evaluation methodology and the evaluation criteria, the description of the lab experiments and the use case based trials in the two pilot cities. Therefore, it will demonstrate the feasibility and reliability of the RERUM architectural framework. It is out of scope to provide good quality final user services from the data collected by RERUM in the applications that the users will interface. The goal is to show that RERUM effectively supports security and privacy by design and that it is scalable as is has incorporated efficiency gains for energy, communications and computation power.

1.2 Intended Audience

The document is intended primarily for the project consortium, namely the researchers, developers that are involved in the technical work packages that will perform the lab experiments, and the pilot cities that will execute the use case trials. However, we believe that the framework can be of interest for researchers and smart city services developers, and the outcomes from the lab experiments and the trials will certainly be of interest for a wider audience, as they will demonstrate the feasibility of the RERUM architecture applied to a live smart city environment.

1.3 Structure

The document is structured as follows:

- Section 2 provides the evaluation methodology that links the development of the architectural framework and the lab experiments and use case based trials to ensure that the architecture provides the expected performance and functionalities. It also provides the evaluation criteria that will be checked in the lab experiments and pilot trials.
- Section 3 sets the proof of concept experiments that will be conducted in simulations and/or controlled laboratory environments in order to qualitatively and quantitatively assess the performance gains of the protocols and algorithms developed within WP2-WP4.
- Section 4 defines field trials for the two pilot cities based on the previously defined use cases. The trials will be performed in two phases. In the first phase one city will test two of the use cases and the other city will test the other two. Before the start of the second trial phase, both cities will exchange the experiences and perform a cross evaluation of the trials from the first phase. In the second phase of the trials the cities will perform the trials of the other two use cases.
- Section 5 provides a checklist of the tests for the RERUM technical contribution.
- Section 6 concludes the document, discussing the main conclusions from the specifications of the trials and the evaluation methodology.

1.4 Relation to other activities and tasks

Deliverable D5.1 is the basis for the work to be performed in WP5 as it defines the tests to perform in the lab experiments and in the trials, as well as the methodology for the evaluation and validation of the results. Task 5.3 will perform the lab experiments defined in section 3, based in the definition of the system architecture from deliverable D2.3. Section 4 details the trials in the two pilot smart cities for the use cases defined in D2.1. Section 4.1 describes the trials that will be performed in Heraklion as part of task 5.4, while section 4.2 describes the trials that will be performed in Tarragona as part of task 5.5. See Figure 1 shows the relationships.

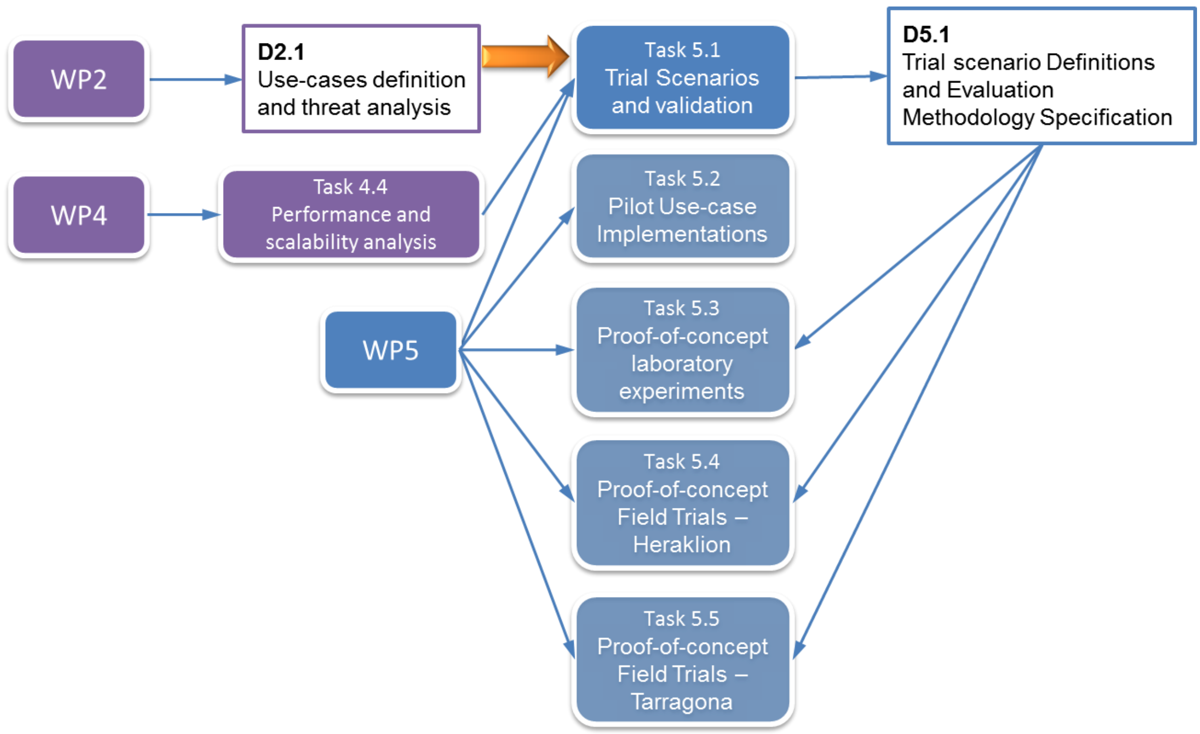

Figure 1 Overview of tasks in WP5 related to D5.1 and the most important links

1.5 Lab experiments and trial activities planning

The planning for the lab experiments and trial activities includes a set of inter-related tasks where some of them provide feedback to other tasks.

Lab experiments, will conduct proof of concept controlled experiments to assess the performance of the components developed within WP2-WP4. The results of these lab tests will be used to improve the components tested, and the conclusions will be applied in the first phase of the live trials in the pilot cities starting in M25. In parallel to the first phase, the lab experiments will continue to improve those components with some performance issues, and the final conclusions and improvements will be provided in M30 just before the start of the second phase of the live trials. The conclusions will be provided in the report *D5.3 Laboratory evaluation*.

Pilot use case implementation task starts at M16 and will run until M24, performing the implementation in terms of development of specific use case components and integration of the trials for the four use cases. Report *D5.2 Smart object and application implementation* provides the specifications of the hardware and software developed for the experiments and trials.

Trials Phase 1 run from M16, performing the preparation activities until M24. These preparatory activities include looking for the optimal location for sensors and devices, distribution of middleware components for each UC in both pilot cities and the planning of the trials activities, and the briefing activities before the live trials start. From M25 until M29 the phase 1 of the live trials is performed, collecting the information to evaluate the performance of the RERUM architectural framework for each UC running in the pilot cities during this phase (UC-O1 & UC-I1 in Heraklion and UC-O2 & UC-I2 in Tarragona).

Trials cross reporting, between M29 and M31, include the debriefing activities from the phase 1 trials, compiling the issues found during the trials (see 2.1.2 Evaluation process, Step 2), the evaluation of the measurements collected during the trials and the users' evaluation results from the surveys. The information collected and the conclusions will be transferred to the other pilot city for the phase 2 trials. As a final step briefing meetings will be hold in each pilot city to the impact from phase 1 results and conclusions to adjust the phase 2 trials accordingly.

Trials Phase 2 run from M25, performing the preparation activities until M30. These preparation activities are equivalent to those described for trials in phase 1. From M31 until M35 the phase 2 of the live trials is performed, collecting the information to evaluate the performance of the RERUM architectural framework for each UC running in the pilot cities during this phase (UC-O2 & UC-I2 in Heraklion and UC-O1 & UC-I1 in Tarragona).

The final step is the **Cross Evaluation** that will collect the results of the two trial phases, analysing the results of the trials in both cities to assess the portability of the RERUM architectural framework. The conclusions will be reported in *D5.4 Field Trials Results & cross evaluation*.

In Figure 2 it is provided a Gantt planning of the activities described above.

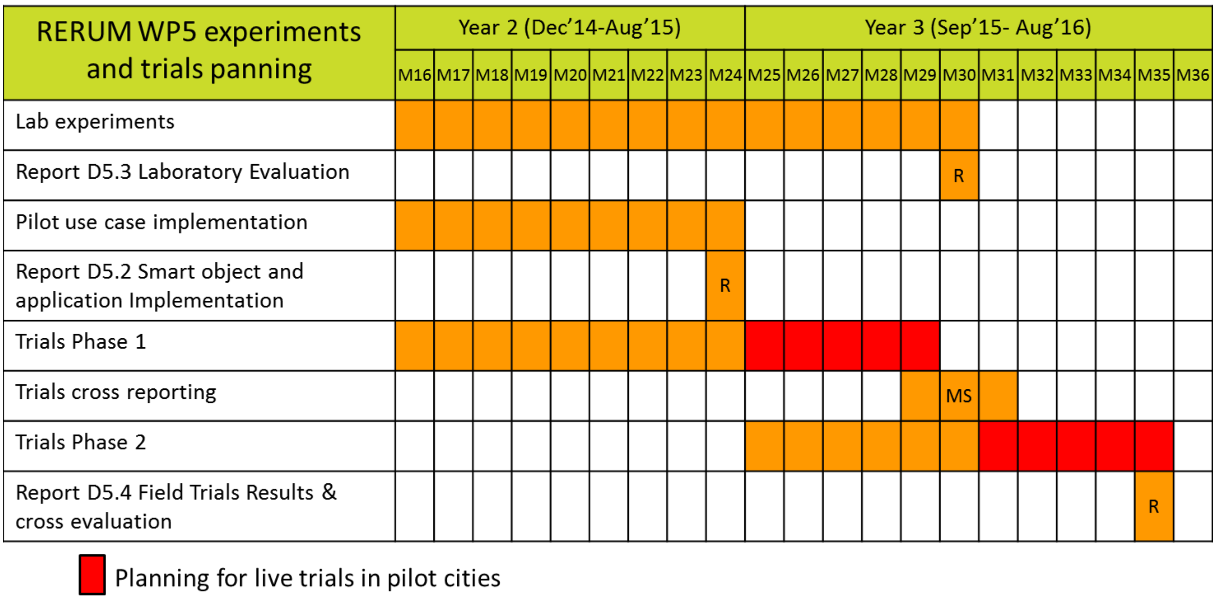

Figure 2 Time plan of lab experiments, use case implementation and trials

Below the approximate planning for trials phase 1 including milestones for meetings and main activities:

- Pre-Trial briefing meetings, for preparation of first phase of live trials by the end of July:
  - During CW 29 to 31 2015 (13^{th} to 31^{st} July 2015)

- Start-trial briefing meetings, to check any issues found after the effective start of live trial, by beginning September when the live trials should start:
    - During CW 37 to 38 2015 (7th to 18th September) - Some follow-up meeting could be necessary.
- Start of the first phase trials: M25- M26 September to October 2015
    - A few RDs will be deployed in strategic points to early detect problems in their performance (data collection, networking, communication with the gateways and the middleware server). The middleware server will be deployed.
- Progressive RDs deployment: M27 - M29 November to January 2016.
    - End-user application deployment. End of the RDs deployment.
- End of trials briefing meeting. To collect information about issues found during trials and evaluation results, by end of January, last month of phase 1 trials:
    - During CW 3 and 4 2016 (18th to 29th January)

2 Evaluation Methodology and Criteria

This section describes the evaluation methodology and the criteria to evaluate the RERUM architectural framework. This evaluation and criteria measures the technical effectiveness, through two different types of tests, *lab experiments* that will test some components and subsystems in a controlled environment, and *trials* that will test the architectural framework in the context of four different use cases in two pilot smart cities. Besides the technical criteria the use cases have specific KPI's to measure the specific performance of the application of the RERUM architecture in real world scenarios, complementary to the evaluation criteria defined later in this section.

2.1 Definition of RERUM evaluation methodology

In the scope of the RERUM project, the evaluation methodology provides the connection between the development of the architectural framework and the lab experiments and use case based trials to ensure that the architecture provides the expected performance and functionalities.

To perform the evaluation the **designers** have provided the evaluation criteria based on the critical innovations of the system, that is, the **target** for the evaluations. These evaluations will be performed by the **evaluators**, partially through in-lab experiments performed by a group of partners which have participated in the design and development of the solution, and through the test trials in both Smart Cities environments considered in the project.

2.1.1 Evaluation model

The ISO has defined a set of series of Standards dedicated to software product quality and evaluation. ISO/IEC14598 [1] series of standards specify the evaluation methodology for general software product in information technology. ISO/IEC9126 [2] series of standards specify metrics for product quality in software engineering and a simplified process for evaluation. These two series of standards are complementary as shown in Figure 3 below.

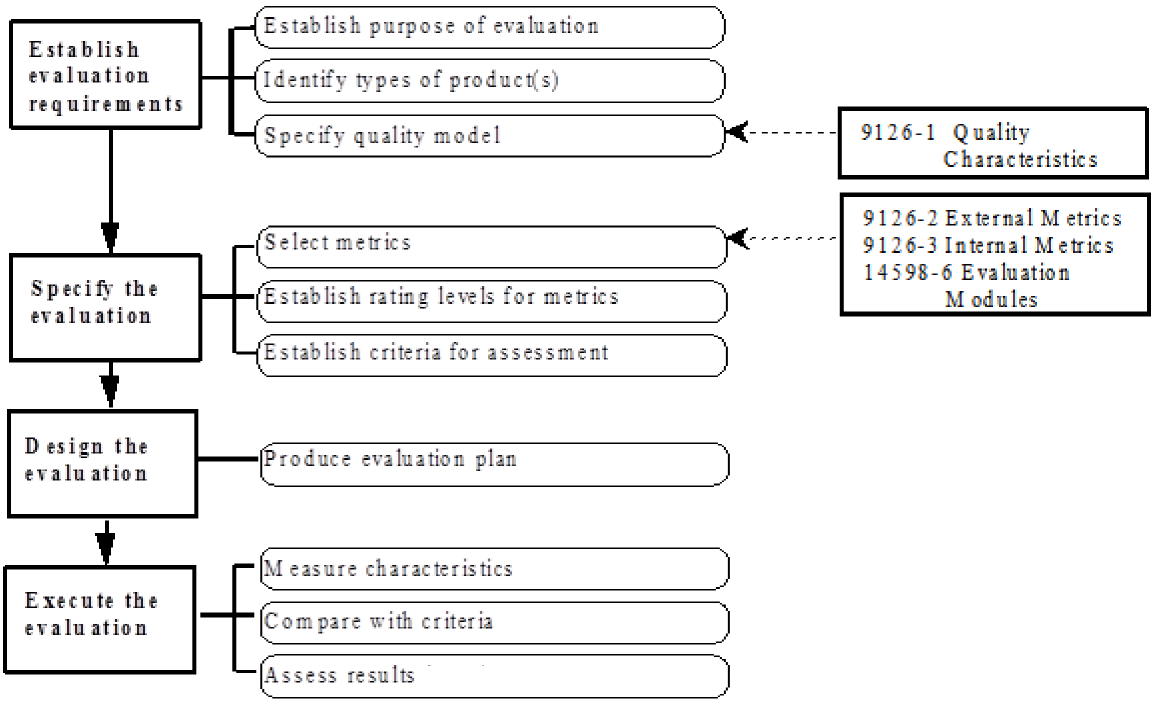

Figure 3 Evaluation process view according to ISO/IEC 14598-1 [4]

Step 1: Establish evaluation requirements

This step establishes the purpose and the products to evaluate, that in the case of RERUM is to test the architectural framework through lab experiments and live trial tests based on previously identified use cases. *The quality model in this case is based on fulfilling the innovation requirements which is the key differentiator of the RERUM platform from other IoT existing architectures*.

Step 2: Specify the evaluation

This step comprises the activities for the selection of metrics, establishing the rating levels and the criteria for assessment.

The quantitative specification and measurement of the software quality requirements can only be made by using metrics which are associated to desired quality characteristics.

For each selected metric evaluation rating values are defined for the related scale, where the required level of the attribute to be measured can be expressed. *Besides the evaluation criteria, each use case has its own KPI's and performance metrics that will provide an evaluation of the impact of each UC in the specific Smart City scenario, besides the RERUM architectural framework*.

For the use case KPI's and performance metrics, when applicable, reference measurements should be considered when these measures compare to situations previous to the deployment of the trials, well based on existing statistics, or performing specific measurements previously to the deployment of the trial use case.

Step 3: Design the evaluation

This step defines the evaluation activities and methods. In RERUM it comprises the in-lab experiments, and the use case trials, where the specific data will be collected to check that the different evaluation criteria meet the evaluation metrics.

Step 4: Execute the evaluation

The selected metrics are applied to the components or solutions, resulting in values on the scales of the metrics. The measured values are then compared to the criteria established in the specification. In the assessment activity a set of rated values are summarised and a statement of the extent to which the software product meets quality requirements is made.

2.1.2 Evaluation process

The approach of evaluation process is composed of three steps, one for the evaluation of the in-lab experiments that will assess the performance of architectural components, a second one to evaluate the overall system on a proof of concept field trials approach, and a third one to perform final cross-evaluation of each UC to assess the portability of the system.

Step 1: In-lab experiments evaluation process. In this process it will be performed the experiments defined in section 3 Proof-of-Concept Laboratory experiments, in a controlled environment, assessing the performance of the specified functionalities. This step will be performed in task T5.3:

1. The results will be measured against the evaluation criteria KPIs defined for each experiment and detailed in section 2.3 Evaluation Criteria.
2. Any deviation from the expected results will be assessed to improve the related system modules or to know their limitations.

3. Any improvement will be incorporated in the modules to be integrated in the trials use cases.

Step 2: Field trials evaluation process. In this process the RERUM architecture will be evaluated with its deployment in different scenarios based on use case descriptions in tasks T5.4 and T5.5:

1. In those use cases with participation of end users, perform the enrolment activities, including necessary open calls for volunteers to be incorporated in the trials.
2. Deployment of the UCs. Including the following activities
    a. Deployment of the integrated components for the use case with the corresponding hardware and software modules.
    b. Training of end users involved in the measures and / or specific users that will monitor the system through the server application or the effective operation of alarms and actuators.
    c. Collect any deployment issues to provide early input to the other city for the second trial phase using the form provided in Annex A.
3. Running the trials to gather information (measurements) defined for each use case, either based on generic or use case specific criteria). Collect any issues during the execution of the trial to provide early input to the other city for the second trial phase using the form provided in Annex A.
4. Evaluation of measurements through the metrics specified for each criterion and against the specified targets.
5. Perform the users evaluation through the specific user satisfaction and acceptance criteria defined for each use case. These evaluations will be performed based on a single specific survey/questionnaire covering all the different user based evaluation criteria for each different type of user.
6. Exchange of evaluation results and the report of trial deployment and execution issues collected during phase 1 trials, with the support of the technical partners to optimise the deployment of the second phase trials.
7. Perform the second phase of the trials for each use case making the improvements recommended by the issues report of the first phase. Execute previous points 1 to 5.

The deployment and execution issues should be collected also during phase 2 of the trials as will be used also for the final cross-evaluation.

Step 3: Cross-evaluation process. This process will receive the results of the two phases of the trials performed in tasks T5.4 and T5.5 and will analyse the results of each city deployment to perform a framework cross-evaluation to assess the portability of the RERUM architectural framework.

1. Collect the evaluation reports and the reports of trial deployment and execution issues from each use case from the two trial phases.
2. Analyse found issues from the collected reports and evaluate if they correspond to:
    a. Specific deployment or execution conditions in one of the trial cities for one of the given use cases. If the issue was only found during the phase-1 trials inquire if this was not found during phase-2 trials because it was avoided after following the recommendations from the reported issue in phase-1 or because the conditions of the trial in phase-2 are different than those in phase-1
    b. Specific deployment or execution conditions in the trial for both cities for one of the given use cases. If the issue was found in both cities, determine, if this was because specific conditions found in both trials or if this issue is independent from those specific conditions, and therefore it will replicate if this scenario is deployed in another Smart City.
3. Analyse evaluation results from measurements and look for deviations from expected targets:

a. For generic evaluation criteria analyse if these deviations are found in one of the following cases to determine if it is dependent from one specific condition in the UC or city or if it is inherent to the architectural framework:
    i. One or more use cases in one city – dependent from a specific city condition
    ii. One or more use cases in both cities – could be inherent to RERUM's architectural framework
b. For use case specific evaluation criteria analyse if these deviations are found only in one city trial or in both to determine if it is dependent from one specific condition in the city or if it is inherent to the architectural framework.
c. Analyse results from users' evaluation, specific for each use case, and look for deviations from expected targets. Analyse if these deviations are found only in one city trial or in both to determine if it is dependent from one specific condition in the city or if it is inherent to the architectural framework.

4. Compile the conclusions from the cross-evaluation process to bring out RERUM's portability to other Smart City use cases or the same tested use cases to other cities.

2.2 Criteria definition template

In this section, we describe fields which will be used to define an evaluation criterion and give a template for criterion definition.

We focus on evaluation criteria from the technical and user perspective or point of view such as performance, security, efficiency, etc.

We identified the following fields to describe an evaluation criterion:

- Identifier: A unique ID number for the criterion (will be assigned later)
- Name: Short name for the criterion
- Category: of the criterion (authorization, efficiency, performance, security)
- Description: Description of the criterion.
- Rationale: brief description explaining why this criterion is important in our evaluation.
- Evaluation responsible: Responsible for performing the evaluation and assuring that the mechanisms to collect the information are in place
- Evaluator - two types of evaluators are defined:
    - Expert: Evaluation performed by a non-final user.
    - User: User based evaluation (can be in addition to the expert based) referring to the usability criteria that will be used for the evaluation.
- Evaluation process: How this criterion must be evaluated:
    - Expert: Description of the expert evaluation process
    - User: Description of the user evaluation process (based on questionnaire or any other form)
- Requirements: Requirements to proceed with the evaluation (availability of hardware, other components, testing conditions)
- Evaluation metrics (KPIs): this field enumerates the evaluation metrics used for the evaluation. The nature depends on the defined criterion. The result of an evaluation criterion can be Boolean (yes/no) or numerical (can be also a percentage). In this case a reference or target value is needed.
- Rank: importance of the criteria; this field is used to specify the importance or ranking of each criterion. For example, each criterion may be assigned a rank of:

    - M: for Mandatory,
    - D: for Desirable, or

  - O: for Optional.
- Type of test: Lab, Trial (or both)

Table 1 below shows the template to complete the criterion definition.

Table 1 Criterion definition template

ID	<unique ID>	Name	<short name>	Category	<category>
Description	<description of the criterion (contribution)>				
Rationale	<brief description for criterion presence>				
Evaluation responsible	<Name of partner responsible>				
Evaluator	Expert; User: { U.Cr.1, U.Cr.7, U.Cr.13, }				
Evaluation process	**Expert**: <how this criterion must be evaluated by experts> **User**: <how this criterion must be evaluated by users>				
Requirements	<requirements to proceed with the evaluation>				
Metrics and target	<KPI and target>				
Rank	<rank>	Type	<Lab, Trial (or both)>		

2.2.1 ID

Every criterion needs to be uniquely identified. The criterion ID is a unique label given to the criterion.

The following naming convention must be followed for all evaluation criteria:

<UC>.<CAT>.<number1>.<number2>.<number3>

Where:

- <UC> indicates the use case concerned by the criterion and can be one of the following:
  - AL = concerns all use cases.
  - ST = Smart transportation (UC-O1)
  - EM = Environmental monitoring (UC-O2)
  - HE = Home energy management (UC-I1)
  - CQ = Comfort quality analysis (UC-I2)
- <CAT> indicates to which category the criterion belongs to. See section 2.2.2 for details.
- <number1>: a unique number of the criterion inside its category. It is a static field.

2.2.2 Category

This field determines the category of the criterion among:

- AU = Authorization;

- EF = Efficiency;
- PE = Performance;
- SE = Security;

This field may be redundant with —ID field since the category information is available in criterion ID.

2.3 Evaluation Criteria

To evaluate the architectural framework the following evaluation criteria are used. Evaluation will be undertaken by:

- Users: It will be based on usability criteria specified in section 2.3.1.
- Experts: The evaluation will be performed by the expert evaluator assigned, either in the lab experiments or in use case trials. Expert-based evaluation will use techniques specific to the criterion being evaluated. The main purpose of these criteria is to evaluate the individual system modules.

Sections 2.3.2 - 2.3.5 specify the details of the criteria being evaluated. For each criterion, the tables list whether it will be evaluated by users and/or experts. They also specify which Use-Cases will be used for the evaluation.

2.3.1 Usability criteria for user-based evaluation

User-based evaluation will be based on questionnaires to be filled in by end-users. The project will leverage the experience with the cooperation with FORSEC (please see section 4.4) for UC-O1. Specifically we will turn to experts to design questionnaires in a format typical for systems' end-users (i.e. rating the level of agreement to statements in a numerical scale). The aim is to get quantitative outputs to criteria as follows:

- Common for all Use-Cases
  - [UE.CO.1]: The application's performance and responsiveness is acceptable and consistent
  - [UE.CO.2]: The application behaves consistently
  - [UE.CO.3]: The application's security features were transparent and did not have a negative impact on its ease of use.
  - [UE.CO.4]: The feature being evaluated, which is experimental and whose utility was being checked in the trial, has proven to be worthy for the user and fulfilled or at least contributed to the objective it was included for.
  - [UE.CO.5]: The users got access to the system according to the security criteria defined by the system administrator
- UC-O1: Smart Transportation
  - [UE.ST.1]: The application had an acceptable impact on my phone's battery life
  - [UE.ST.2]: The application had a positive impact on my transportation planning.
  - [UE.ST.3]: The application resulted in a change of my transportation habits.

2.3.2 Authorization criteria

ID	AL.AU.1	Name	Enrich authorization process with reputation evaluation	Category	Authorization, Reputation

Description	Enrich authorization process with reputation evaluation. This trial is a special one. The trust model and the reputation engine of RERUM is meant to evolve with the evaluation of the users. In fact, Task 3.4 lasts till the second round of the trials for this reason
Rationale	Check that the addition of the reputation evaluation really makes a useful difference by looking for cases where it changes the result of the access decision. This trial is based on the interaction with the user to refine progressively the trust model of RERUM. For this reason, it does not aim to have a high percentage of successful evaluations at first. Instead, It aims to take into account the feedback from the users to refine this evaluation. This trial will be considered a success if the trust engine gets improved due to the feedback provided by the user and if the system administrator finally decides that it is worth to keep on using the reputation evaluation on the authorization decision.
Evaluation responsible	ATOS
Evaluator	Expert; User: {UE.CO.1, UE.CO.2, UE.CO.3, UE.CO.4, UE.CO.5}
Evaluation process	**Expert:** 1. Upload a policy in the system that allows all guest user to access the system if their reputation is higher than normal 2. Citizens that has not provided mobility data yet try to access android application to collect mobility information 3. The reputation engine evaluates the reputation of these citizens. At least one of these citizens gets a reputation ratings lower than good. Note that the evaluation of the reputation might depend on more factors decided by the system administrator during the trial. Hence it is not necessarily true that all these evaluation will result in a rating lower than good. The result of the evaluation gets reflected in the log 4. These volunteers with reputation ranking lower than good do not get access to the mobility data. The result of the access is reflected in the logs 5. Citizen volunteers provide mobility data 6. The reputation of these volunteers get a bonus due to their contribution, which is also reflected in the application logs 7. Citizen volunteers try to access android application to collect mobility information 8. The reputation engine evaluates the reputation of these citizens. At least one of these citizens gets a good reputation rating. Note that the evaluation of the reputation might depend on more factors decided by the system administrator during the trial. Hence it is not necessarily true that all these evaluation will result in a high ranking. The result of the evaluation gets reflected in the log 9. The volunteer with good reputation ranking gets access to the mobility data. The result of the access is reflected in the logs 10. Check whether the access decision changes **User: System administrator** 1. Discuss trust model with expert and provide feedback to him 2. User (administrator): Decide on whether to keep the policy that takes into account the evaluation of the reputation or not 3. User (non-municipality users known to have a reputation evaluation subject to change the decision): Try to access the system with the different policies active
Requirements	Citizens' volunteers must not have assigned any role related with the municipality while performing this evaluation.
Metrics and target	The key target here is that there is at least one real user that gets its access altered by this metric Target 1: The reputation engine properly evaluates the reputation for all the volunteers

<table>
<tr><td></td><td colspan="3">Target 2: Number of policies taking into account the evaluation of the reputation result kept by the administrator user at the end of the trial > 0</td></tr>
<tr><td>Rank</td><td>D</td><td>Type</td><td>Trial (UC: I1, I2, O1)</td></tr>
</table>

<table>
<tr><td>ID</td><td>AL.AU.2</td><td>Name</td><td>Integration of ABAC in IoT with business data</td><td>Category</td><td>Authorization</td></tr>
<tr><td colspan="2">Description</td><td colspan="4">Integration of ABAC in IoT with specific business data contained in the attributes of the user that is issuing the request</td></tr>
<tr><td colspan="2">Rationale</td><td colspan="4">The user attributes are provided by the identity provider and are normally paramount in the access decision, because of being guaranteed by the Identity provider himself. This test checks the ability of the system to make decisions based on those attributes</td></tr>
<tr><td colspan="2">Evaluation responsible</td><td colspan="4">ATOS</td></tr>
<tr><td colspan="2">Evaluator</td><td colspan="4">Expert; User: { UE.CO.1, UE.CO.2, UE.CO.3, UE.CO.5}</td></tr>
<tr><td colspan="2">Evaluation process</td><td colspan="4">Expert:
1. Define a user attribute in the Identity platform or make sure that you use an already existing one in the following step
2. Upload in the system at least 1 security policy that makes use of this attribute in the access decision. For instance, use a role attribute to check that the user is assigned that role
3. Check the policy with different users that have different values for that attribute by inspecting the logs of the authorization engine
User (administrator):
Using a set of previously known users with known values for the attribute being taken in consideration for the evaluation of the policy, check they get granted access to the application accordingly to their attributes. Take note on the total number of accesses and any wrong access to it.
Reset the number of wrong accesses and wrong accesses to zero if a fix regarding this is provided.</td></tr>
<tr><td colspan="2">Requirements</td><td colspan="4">None</td></tr>
<tr><td colspan="2">Metrics and target</td><td colspan="4">Number of wrong accesses to the system according to this policy = 0
Number of non-test policies referring to user attributes > threshold
Target threshold to be defined by the municipality. Value recommended = 0</td></tr>
<tr><td colspan="2">Rank</td><td colspan="2">M</td><td>Type</td><td>Trial (UC: O1, O2, I1, I2)</td></tr>
</table>

<table>
<tr><td>ID</td><td>AL.AU.3</td><td>Name</td><td>Integration of ABAC in IoT with system attributes</td><td>Category</td><td>Authorization</td></tr>
<tr><td colspan="2">Description</td><td colspan="4">Integration of ABAC in IoT with system attributes</td></tr>
<tr><td colspan="2">Rationale</td><td colspan="4">Check that the system is able to make access decisions based on the day or hour of the request</td></tr>
</table>

Evaluation responsible	ATOS		
Evaluator	Expert; User: { UE.CO.1, UE.CO.2, UE.CO.3, UE.CO.4, UE.CO.5}		
Evaluation process	**Expert**: Prepare 2 XACML policies that take into account the date and time of the request, respectively, and check they work properly by executing operations through the applications at distinct hours and days to cover the four possible combinations of date / time with available and non-available slots. Specifically, create policies that take into account time ranges where special environmental conditions are expected, such as Tarragona's annual Firework contest **User (System administrator):** Check that the final users get properly authorized depending on the date / times they access to the system		
Requirements	These tests require to be executed at certain hours of the day to make sure they are evaluated properly		
Metrics and target	Percentage of correct evaluations = 100 Number of non-test policies containing time or date criteria > threshold Target threshold to be defined by the municipality. Value recommended = 0		
Rank	D	Type	Trial (UC: O2)

ID	AL.AU.4	Name	Integration of ABAC in IoT with specific business data in the request	Category	Authorization
Description	Integration of ABAC in IoT with specific business data contained in any text information contained in the request, even if its structure is specific from the resource or service to be accessed. More specifically, this evaluation checks that the requests contain a field that indicates the requester has accepted the privacy conditions needed to access the service				
Rationale	Check the ability of the system to evaluate any text content of the request in any of the supported MIME-TYPE formats				
Evaluation responsible	ATOS				
Evaluator	Expert; User: { UE.CO.1, UE.CO.2, UE.CO.3, UE.CO.5}				
Evaluation process	**Expert in collaboration with service developer**: 1. Prepare a requests that contain a check on the field that checks the acceptance by the requester of the privacy conditions needed to access the service 2. Upload proper XACML policies that evaluate that concrete field independently 3. Check that they are evaluated correctly. **User (System administrator):** Check that the user get properly authorized depending on whether they have accepted the privacy conditions or not				
Requirements	In this concrete case, the evaluation is specific to the structure of the request, which is				

	known by its developer or the system administrator. For this reason, it is necessary that this test is checked not only by the security expert but also by the developer of the service to be protected. It will also be necessary to have complete documentation of the API that each service is exposing.		
Metrics and target	Percentage of correct evaluations = 100 Number of non-test policies containing any supported fields > threshold Target threshold to be defined by the municipality. Value recommended = 0		
Rank	D	Type	Trial (UC: O1)

ID	AL.AU.5	Name	Integration of ABAC in IoT with specific business data in predefined attribute purpose	Category	Authorization
Description	This evaluation criteria checks that the system is effectively able to enforce privacy criteria based on purpose parameter				
Rationale	Purpose is a paramount attribute when it comes to enforce privacy criteria because PbD is based on the purpose that the data are going to be used for. For this reason, all requests are required to include a purpose field stating it. The tests in this table check that the System is able to take into account the purpose stated in the request and in the privacy policies to grant or reject access to the RERUM services.				
Evaluation responsible	Atos				
Evaluator	Expert; User: { UE.CO.1, UE.CO.2, UE.CO.3, UE.CO.4, UE.CO.5}				
Evaluation process	**Expert**: 1. For UCO1: Upload a privacy policy that checks that the field purpose has a value of 'Mobility Application' 2. For UCI2: Upload a privacy policy that checks that the field purpose has a value of 'Statistics' 3. For each use case, issue requests that would be accepted if this criteria would not be taken into account and vary the field purpose. Those requests that have the value 'Mobility Application' for UC01 or 'Statistics' for ICI2 must be accepted and the rest must be rejected **User (System administrator):** Check that the data to be protected by those policies can be accessed only through the actions in the applications that corresponds with the ones defined in the privacy policies and count any possible access not complaining with that purpose.				
Requirements	The application developers will have to provide examples of valid requests to their services so It is possible for the expert to tweak the field 'purpose' manually				
Metrics and target	Percentage of correct evaluations = 100 Target: Number of accesses to these data that get granted but do not comply with the consent expressed in the policy policies = 0				
Rank	D	Type	Trial (UC: O1, I2)		

ID	AL.AU.6	Name	Ability of the administrators to create their own security criteria	Category	Authorization
Description	This evaluation criteria checks that the administrator is effectively able to define and upload his own security criteria to the system				
Rationale	RERUM provides an extremely authorization engine based on XACML policies. However, XACML is a very complex language and user administrators are not prone to know it, at least at its full power. For this reason, the RERUM prototype includes an API that allows for the automatic creation of XACML policies without any XACML knowledge. The applications are meant to provide a GUI to invoke this API so an administrator can easily create the XACML policies on his own.				
Evaluation responsible	Atos				
Evaluator	Expert; User: { UE.CO.1, UE.CO.2, UE.CO.3, UE.CO.4}				
Evaluation process	**User (System administrator):** Helped by the expert and the GUI, the user is meant to be able to create his own XACML files or to deploy already advanced ones. In order to do so, he will: 1. Define the security criteria at a logical level with the help of the expert 2. Create a valid XACML policy using the GUI according to the defined security criteria 3. Upload the newly created policy 4. Check that the policy properly evaluates the access to the system The expert will provide technical consultancy to the system administrator about the logical criteria needed to build the XACML policies on his own, but will not build the XACML policies				
Requirements					
Metrics and target	Target: Number of XACML policies created and deployed by the System Administrator > 0				
Rank	D	Type	Trial (UC: O1, I2)		

2.3.3 Efficiency criteria

ID	ST.EF.1	Name	Power Consumption rates (Android)	Category	Efficiency, Energy
Description	The criterion aim is to measure the battery consumption of the developed android apps once the RERUM middleware is used with them.				
Rationale	The android application must be lightweight in battery consumption so that citizens have very limited to no observable battery drain when installing and running it.				
Evaluation responsible	LiU				
Evaluator	Expert at Lab User at Trial				
Evaluation process	To evaluate the power consumption standard programming tools within the android suite exist. In lab there will be a set of experiments where the developed apps will be tested. (see: https://source.android.com/devices/tech/power.html) Private user should answer question on observing significant battery depletion times after installing the UC-O1 trial app.				
Requirements	Android devices that include a battery fuel gauge such as a Summit SMB347 or Maxim MAX17050.				
Metrics and target	Loss of battery % per operational hour, per operation session				
Rank	M	Type	Lab & Trial (O1)		

ID	ST.EF.2	Name	CPU Load of mobile device	Category	Efficiency, Resources
Description	The criterion aim is to measure the CPU load of the developed android apps once the RERUM middleware is used with them.				
Evaluation responsible	LiU				
Rationale	The android application must be lightweight in CPU usage so that citizens have very limited to no observable processing burden when installing and running the apps				
Evaluator	Expert at Lab User at Trial				
Evaluation process	To evaluate the CPU load programming tools within the android API are available: for example the Android System Monitor is a system-level monitor tool for Android system. It can real-time display and record system information (ex: CPU, memory usage, network etc.). It also provides APIs for more accurate measurement. Private user should answer question on observing significant glitches in the Quality of				

	Experience when the app is not in the foreground after installing the UC-O1 trial app.		
Requirements	-		
Metrics and target	Keep the CPU % of the app as low as possible while collecting and transmitting		
Rank	M	Type	Lab & Trial (O1)

ID	AL.EF.3	Name	Crypto-Memory-Consumption-Overhead	Category	Efficiency, Resources
Description	• ECC Signature on device to have a secure integrity SA from the RERUM device • Lightweight Datagram Transport Layer Security (DTLS) Protocol • Malleable Signatures on device to allow and control authorised modifications				
Rationale	This criterion evaluates the increase in memory consumption (RAM, ROM, external storage) when the RERUM devices or other platforms are executing a specific cryptographic algorithm or protocol by which RERUM wants to enhance the security. This allows assessing if the specific cryptographic algorithm or protocol is suitable for running on a constrained device, with limited storage in RAM and ROM. Using additional space on external memory will negatively affect the energy efficiency and the speed.				
Evaluation responsible	UNIVBRIS for: • Lightweight Datagram Transport Layer Security (DTLS) Protocol UNI PASSAU for: • ECC Signature on device to have a secure integrity SA from the RERUM device • Malleable Signatures on device to allow and control authorised modifications				
Evaluator	Expert at lab				
Evaluation process	**Expert**: • Rough estimation based on compiled code size and/or the required memory for storing cryptographic keys • Prototypical implementations on platforms (e.g. Z1, RE-Mote, OpenMote, RaspberryPI, etc.) can be measured using compiler options and runtime monitors.				
Requirements	• Cryptographic algorithms parameters regarding type of keys and key size • Hardware and prototypical implementation				
Metrics and target	• Average memory Consumption (RAM, ROM and external storage) of a specific crypto algorithm (in bytes) • Overhead (additional memory Consumption (RAM, ROM and external storage)) of an interaction involving the cryptographic algorithm (e.g. encrypting a message and sending the encrypted message) compared to the same interaction not involving the cryptographic algorithm (e.g. sending the plain text message).				
Rank	M		Type	Lab	

ID	AL.EF.4	Name	Crypto-Communication-Overhead	Category	Efficiency, Communication
Description	• ECC Signature on device to have a secure integrity SA from the RERUM device • Lightweight Datagram Transport Layer Security (DTLS) Protocol				

	• Malleable Signatures on device to allow and control authorised modifications		
Rationale	This criterion evaluates the increase in message sizes or communication activity (message size, number of messages) when the RERUM devices or other platforms are executing a specific cryptographic algorithm or protocol by which RERUM wants to enhance the security. This allows assessing if the specific cryptographic algorithm or protocol is suitable for running on a constrained device, with limited energy for sending messages wirelessly. An increased length of communication messages or the need for additional messages will negatively affect the energy efficiency.		
Evaluation responsible	UNIVBRIS for: • Lightweight Datagram Transport Layer Security (DTLS) Protocol UNI PASSAU for: • ECC Signature on device to have a secure integrity SA from the RERUM device • Malleable Signatures on device to allow and control authorised modifications		
Evaluator	Expert at lab		
Evaluation process	**Expert**: • Rough estimation based on theoretical handshakes of protocol, and theoretical size of messages exchanged • System simulations can be used for evaluating the number of messages • Prototypical implementations on platforms (e.g. Z1, RE-Mote, OpenMote, RaspberryPI, etc.) can be measured using debug output and network monitoring equipment (sniffers).		
Requirements	• Cryptographic algorithms parameters regarding protocol and message flows and used primitives and their security parameters (size of keys, length of hash, etc.) • Hardware and prototypical implementation		
Metrics and target	• Average increase in message size of a specific crypto algorithm (in bytes) • Average number of messages of a specific crypto algorithm (natural number) • Overhead (additional number of messages or additional message size) of an interaction involving the cryptographic algorithm (e.g. encrypting a message and sending the encrypted message) compared to the same interaction not involving the cryptographic algorithm (e.g. sending the plain text message).		
Rank	M	Type	Lab

ID	AL.EF.5	Name	Crypto-Energy-Consumption	Category	Efficiency, Energy
Description	• ECC Signature on device to have a secure integrity SA from the RERUM device • Lightweight Datagram Transport Layer Security (DTLS) Protocol • Malleable Signatures on device to allow and control authorised modifications				
Rationale	This criterion evaluates the increase in message sizes or communication activity (message size, number of messages) when the RERUM devices or other platforms are executing a specific cryptographic algorithm or protocol by which RERUM wants to enhance the security.				
Evaluation responsible	UNIVBRIS for: • Lightweight Datagram Transport Layer Security (DTLS) Protocol UNI PASSAU for: • ECC Signature on device to have a secure integrity SA from the RERUM device • Malleable Signatures on device to allow and control authorised modifications				

Evaluator	Expert at lab
Evaluation process	**Expert**: • System simulations if the energy usage for messages and transmission of a certain length are known and the protocol can be simulated inside a simulation framework • Prototypical implementations on platforms (e.g. Z1, RE-Mote, OpenMote, RaspberryPI, etc.) and measuring it using either the powertrace module of Contiki or using special hardware
Requirements	• Cryptographic algorithms parameters regarding protocol and message flows and used primitives and their security parameters (size of keys, length of hash, etc.) • Hardware and prototypical implementation
Metrics and target	• Average increase in energy consumption of a specific crypto algorithm (in mWh) • Overhead (additional mWh) of an interaction involving the cryptographic algorithm (e.g. encrypting a message and sending the encrypted message) compared to the same interaction not involving the cryptographic algorithm (e.g. sending the plain text message).
Rank	M | Type | Lab

ID	AL.EF.6	Name	Adaptive compressive sensing encryption/compression	Category	Efficiency, Energy
Description	• Secure and energy efficient data encryption/compression • Adaptive compression based on the required QoS				
Rationale	The aim is to evaluate the performance and the efficiency of the adaptive CS-based data gathering mechanism that has been developed within RERUM. This mechanism aims to provide a secure and energy-efficient way of gathering sensing measurements from constrained IoT devices that can provide services with different Quality of Service (QoS) requirements.				
Evaluation responsible	FORTH				
Evaluator	Expert				
Evaluation process	**Expert**: • Three RERUM devices will be used (transmitter, receiver, gateway) • Data encryption/compression at the transmitter • Data decryption/decompression at the receiver • Reconstruction error estimation at the receiver, and new compression rate computation, if needed, for meeting the desired QoS				
Requirements	• Software implementation of the adaptive CS in the RERUM devices • Data storage in the RERUM devices				
Metrics and target	• Reconstruction error at the receiver • Percentage of time the reconstruction error stays above the threshold defined by the QoS of the provided service class • Energy consumption of this technique compared with the energy consumed when transmitted uncompressed measurements • Time required to detect changes in the signal sparsity and adapting to a new compression rate • False alarms/misdetections in sparsity changes • Communication overhead (increased signalling) for adapting to the sparsity changes				

Rank	O	Type	Lab

2.3.4 Performance criteria

ID	ST.PE.1	Name	App. & Server Uptime & Crash Frequency	Category	Performance, Scalability
Description	The criterion measures uptime of the developed android apps once the RERUM middleware is used with them.				
Rationale	The aim to catch at the lab any potential bugs that may hinder the application implementation in the trial				
Evaluation responsible	LiU				
Evaluator	Expert at Lab User in UC-O1 Phase 2				
Evaluation process	The test application will report whenever crashes occur and this will be a repeated experiment on every major revision released in the project within the application development process. Users will evaluate by answering a question regarding how often they got error messages that required them to re-start the app.				
Requirements	N/A				
Metrics and target	The target is to investigate whether the app uptime that is independent of network and load				
Rank	D	Type	Expert in Lab Users in trial (UC: O1)		

ID	AL.PE.2	Name	Measurement precision	Category	Performance
Description	This criterion measures the variance around the mean of a collected value in a given static scenario				
Rationale	The aim is to identify the precision (confidence interval) of a limited number of measurements, when there can be no ground truth.				
Evaluation responsible	LiU				
Evaluator	Expert at Lab				
Evaluation process	Long-term (order of hour) measurements will be taken at static locations. Statistics will be taken and the precision (variance) and confidence interval of the measured quantity will be				

	drawn.		
Requirements	N/A		
Metrics and target	The metric is measurement variance around the mean over a window of time. The target is to have it as close to the mean.		
Rank	D	Type	Lab

ID	AL.PE.3	Name	Crypto-Runtime-Overhead	Category	Performance
Description	• ECC Signature on device to have a secure integrity SA from the RERUM device • Lightweight Datagram Transport Layer Security (DTLS) Protocol • Malleable Signatures on device to allow and control authorised modifications				
Rationale	This criterion evaluates the performance in terms of speed when the RERUM devices or other platforms are executing a specific cryptographic algorithm or protocol by which RERUM wants to enhance the security. This allows assessing if the specific cryptographic algorithm or protocol is suitable for running on a constraint device, with limited storage in RAM and ROM. The speed will determine for which types of scenarios this algorithm is suitable.				
Evaluation responsible	UNIVBRIS for: • Lightweight Datagram Transport Layer Security (DTLS) Protocol UNI PASSAU for: • ECC Signature on device to have a secure integrity SA from the RERUM device • Malleable Signatures on device to allow and control authorised modifications				
Evaluator	Expert at Lab				
Evaluation process	**Expert**: • Algorithm and System simulations can be used for the evaluation of the required clock-cycles and clock speeds of platforms • Prototypical implementations on platforms (e.g. Z1, RE-Mote, OpenMote, RaspberryPI, etc.) can be measured using time stamping of several runs of the algorithms and taking the mean.				
Requirements	• System parameters and availability of a Simulation framework • Hardware and prototypical implementation				
Metrics and target	• Runtime of average execution time of a specific crypto algorithm (in milliseconds) • Overhead (additional execution time) of an interaction involving the cryptographic algorithm (e.g. encrypting a message and sending the encrypted message) compared to the same interaction not involving the cryptographic algorithm (e.g. sending the plain text message).				
Rank	M		Type	Lab	

ID	AL.PE.4	Name	Lightweight Datagram Transport Layer Security (DTLS) Protocol	Category	Performance
Description	Investigation of DTLS protocol in a real deployment setup.				

Rationale	There are many undefined factors of a lightweight DTLS implementation especially considering real deployment behaviour. It is important to select cryptographic schemes that will yield to the best performance at chosen security level. As the best performance (i.e. trade-off between factors) one can think of algorithm speed, code footprint or power consumption and all these metrics will be investigated in the experiment. There is also a need to investigate the impact of cryptographic primitives onto the overall protocol performance.
Evaluation responsible	UNIVBRIS
Evaluator	Expert at Lab
Evaluation process	**Expert**: • Code footprint will be measured at compile-time during lab experiments. • Performance of particular cryptographic primitives, as well as overall DTLS performance will be measured using on-device timer with specially adjusted DTLS code during a run-time. • Power consumption will be measured by external special purpose hardware; DTLS code will be adjusted to provide said measurement possibility.
Requirements	• Four Re-Mote platforms and one Gateway, connected to each other in specific network topology. • Implementation of DTLSv1.2 protocol. • Implementation of selected cryptographic primitives, adjusted to Re-Mote and Gateway platforms. • Equipment to measure power consumption on Re-Motes during a run-time.
Metrics and target	• Code footprint of cryptographic primitives. • Performance of cryptographic primitives running on both Re-Mote platform and Gateway. • Power consumption of cryptographic primitives, as well as overall power consumption of DTLS protocol. • Overall latency of DTLS handshake in different scenarios, i.e., using symmetric and asymmetric schemes in end-to-end scenario.
Rank	M | Type | Lab

ID	AL.PE.5	Name	6LoWPAN Multicast	Category	Performance
Description	To demonstrate how M/W functions can leverage layer 3 multicast in order to improve network performance and decrease energy consumption, ultimately increasing deployment lifetime.				
Rationale	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.		
Evaluation responsible	UNIVBRIS		
Evaluator	Expert at Lab User in UC-O2 and UC-I1, based on UE.CO.1, UE.CO.2, UE.CO.3		
Evaluation process	**Expert**: Code footprint and RAM requirements will be measured at compile-time during lab experiments. For the remaining metrics: • A set of RDs will subscribe to a multicast group. • A RERUM gateway will be selected as the source of multicast traffic, with destination to this multicast group. Different experiments will use different characteristics for this traffic, in terms of inter-packet interval, packet size, bit-rate (Constant vs Variant). For each of those permutations: • Network Delay will be evaluated by measuring Round-Trip-Time (RTT) • Reliability will be evaluated by measuring Packet Delivery Ratio on each multicast group subscriber. **User**: User evaluation will be undertaken as per section 2.3.1		
Requirements	Due to restrictions discussed in D2.1, evaluation will require that the software process generating multicast traffic be executed on the RERUM gateway (see D2.1, Sec 4.2, Contribution 22)		
Metrics and target	• Reliability by measuring packet loss / packet delivery ratio. Target: This metric is highly-sensitive to traffic rate, network topology, node configuration etc. Therefore, it will be evaluated through comparisons with current state-of-the-art. • Network Delay (<1 sec per network hop) • Suitability for embedded devices by measuring code size and RAM requirements. Targets for the RE-Mote platform: <3 KB and <3 KB respectively)		
Rank	D	Type	Lab, Trial (UC: O2, I1)

ID	AL.PE.6	Name	Compressive sensing encryption/compression	Category	Performance
Description	To demonstrate the efficiency for extracting encryption and compression keys that are used for Compressive Sensing in a real-world experiment.				
Rationale	Secret key establishment is a fundamental requirement as wireless sensor networks carry sensitive and private information over unattended environments. As sensors are severe resource constrained devices, energy efficient cryptographic algorithms are a necessity. Typical key generation algorithms have several inefficiencies like requiring a key distribution mechanism, need to pre-store the keys on the devices, etc. In the foreseen experiments, the RERUM devices will create their encryption keys based on channel measurements, and more specifically, using the Received-Signal-Strength-Indicator (RSSI).				

Evaluation responsible	FORTH		
Evaluator	Expert		
Evaluation process	**Expert**: • Three RERUM devices will be used. • Two of them acting as legitimate devices and one as a malicious one • Initially, the legitimate devices will exchange packets in order to create the encryption keys • The malicious device will overhear the wireless medium executing the same key generation algorithm		
Requirements	• Software implementation of the secret key generation algorithm in the RERUM devices • Data collected on the devices and post-processed in Matlab		
Metrics and target	• Bit mismatch rate between the encryption keys of the legitimate and the malicious devices • Reconstruction error at the two receivers • Time required to agree upon a common secret key		
Rank	O	Type	Lab

ID	AL.PE.7	Name	Lightweight spectrum sensing and spectrum assignment	Category	Performance
Description	To demonstrate the efficiency of the lightweight spectrum sensing and spectrum assignment frameworks				
Rationale	The purpose of the spectrum sensing module is to allow the Cognitive Radio-based RDs to be able to gather spectrum occupancy statistics in an energy efficient way and then extract models of the spectrum occupancy of specific bands. This will minimize the energy consumed by the RDs for sensing the available spectrum bands, by extracting an optimum period for sensing each band and avoid sensing the bands very frequently (process that consumes a lot of energy). The purpose of the spectrum assignment module is to allow the Cognitive Radio-based RDs to select the most appropriate and suitable spectrum band for meeting the transmission requirements of the service class(es) it provides. A basic target in this spectrum assignment mechanism is to meet the QoS requirements of the service class and to select the most suitable spectrum, in terms of optimal central frequency and band width for this transmission and all these with an objective to consume a minimum amount of energy.				
Evaluation responsible	FORTH				
Evaluator	Expert				
Evaluation process	**Expert**: Two SDR devices will be used. A spectrum band will be selected and monitored with the spectrum assignment mechanisms installed. The goal is to learn the transmission pattern of the licensed users (the licensed user will be emulated with a second SDR).				

Requirements	• An SDR will be used for spectrum sensing/assignment • A second SDR will be used for primary used emulation (in TV bands)		
Metrics and target	• Speed of convergence to the optimum period for spectrum sensing. • Energy consumed for sensing until the convergence is reached. • Energy consumed for sensing using the optimum period. • Scalability of the mechanism when the number of the available spectrum bands that the RD senses increases. • Power consumption for transmitting at the selected frequency/bandwidth.		
Rank	O	Type	Lab

ID	EM.PE.8	Name	Device availability	Category	Performance
Description	Provide availability information of deployed devices to allow users and maintainers to assert the deployment status, schedule preventive maintenance if one or more devices shows behaviours prone to failure, and to provide users and services exploiting the data reliability criteria.				
Rationale	The users and maintainers of deployments and running applications expects a reliability criteria, to assert the smart devices operation, this builds trustworthy and reflects transparency of provided services.				
Evaluation responsible	Zolertia				
Evaluator	Expert				
Evaluation process	The RD are to be deployed on site. The maintainer or installer is to restart the counters as soon as there are at least 5 received packets on the server-side. If a RD fails to send any packet at this time, is to be addressed individually. Logs and graphs are to be stored periodically on a daily or weekly basis. Uptime breakdowns of RD are to be diagnosed using available status information (RSSI, battery level, etc.), and documented in the deployment log.				
Requirements	Information about the RD uptime (seconds elapsed since boot) and message counter sent as metadata periodically. Information about the RD battery life, link quality, RSSI and next-hop parent (in a mesh-like network) sent as metadata periodically. This information shall be used to diagnose possible causes of availability loss. The RD should periodically send keep-alive messages with the above information to the Server-Side application, if no periodical information is to be sent from the RD, i.e. in an event-based or alarm application. The server-side application should keep a counter of received and expected messages from every RD. The server-side application should store the historical values of the uptime value of each RD, and be able to distinguish when receiving a counter value of 1 (starting value) due to a counter wrap-around (32-bit variable width suggested), or because of i.e. a RD reboot. The server-side application should display the uptime and packet reception rate				

	information graphically or in tables, with a timestamp reference appended at packet reception at the server-side. The server-side application should support resetting the stored values (uptime, counters, etc.), to allow the maintainer and installer to restart the application, for example upon deployment of the system. The expected uptime per RD should start ticking with a 1 second period when received a first packet from a RD, or upon an application restart as described above. The server-side application should display an alarm about a RD being unavailable, if the RD's PRR drops below a given percentage (to be configured by the maintainer at the deployment phase), providing also a timestamp of the time of the occurrence.		
Metrics and target	The target are users affected by the system being unavailable, also requiring metrics and statistics to validate the system availability and performance, to schedule maintenance tasks, deployment of services using the information provided by the RDs, etc. The following KPI are to be used: PRR (packet reception rate) per RD. Uptime ratio = RD uptime (sum of seconds elapsed) / RD expected uptime. Restart Ratio = number of boot or reboots/day		
Rank	D	Type	Trial (UC-O2)

2.3.5 Security criteria

ID	AL.SE.1	Name	SIEM	Category	Security, Monitoring
Description	SIEM in a generic IoT platform				
Rationale	Monitoring and analysing the logs and events in the system 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.				
Evaluation responsible	ATOS				
Evaluator	Expert				
Evaluation process	**Expert**: • Visualising in the SIEM web interface, the list of events coming from a RERUM data source previously collected by the SIEM Agents. • Simulate (generate entries in the data source -log file-) a sequence of events that complains with a predefined correlation rule that generates an alarm. • Visualising in the SIEM web interface, in the alarms section, an alarm caused by RERUM events. • Check that a simple action like send an e-mail or execute a simple command is done and caused by the alarm.				
Requirements	• SIEM server installed • SIEM agent installed • Plugin configured in the agent for capture the logs from a specific data source. • Define a correlation rule in the server that triggers an alarm when a concrete				

	sequence of RERUM events is detected. • Define an action in SIEM server • Create a policy that associates the alarm and the action.		
Metrics and target	The target is the storage of RERUM events and alarms and detection of a concrete behaviour based on events and reacts on run-time. Those events and alarms helps to know to administrators what is happened in the RERUM network and gives information for decision taking.		
Rank	M	Type	Trial (UC: O2, I1, I2)

ID	AL.SE.2	Name	React to alert	Category	Security, Automation
Description	Incorporating adaptability to an IoT platform using PRRS and OAP / react to SIEM event				
Rationale	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 context information coming from the events monitoring is key importance for taking the appropriate action.				
Evaluation responsible	ATOS				
Evaluator	Expert				
Evaluation process	**Expert**: • Send an alarm (automatically via SIEM Action or manually) sending an HTTP POST with the alarm in JSON format to the PRRS endpoint: '/PRRS-services/resources/alarms' • Check with a GET to the same endpoint if the Alert is listed as received. • Check with a GET to the endpoint '/PRRS-service/resource/actionstaken' where will be a list of entries with the last actions taken, its associated alarms and the result of each action.				
Requirements	• PRRS tool installed and accessible in port http 8080. • Define the set of context variables that we can use in the PRRS rule designer. • Define a set of PRRS rules, using the PRRS rule designer in the endpoint '/PRRS-webgui', to deal with the alarms that we want to address.				
Metrics and target	Demonstrate that the system is able to use context information coming from a system alarm and take it into account for taking actions to mitigate the problem that caused the alarm. The results of the actions taken are accessible from the PRRS interface to check them.				
Rank	D	Type	Trial (UC: O2, I1, I2)		

ID	AL.SE.3	Name	React to context change	Category	Security, Automation
Description	Incorporating adaptability to an IoT platform using PRRS and OAP / react to security criteria				
Rationale	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 context information coming from system's monitors or the expertise of system administrators is a valuable asset for taking				

	the appropriate action.		
Evaluation responsible	ATOS		
Evaluator	Expert		
Evaluation process	**Expert**: • Change the value of a predefined context variable (manually or provided by a connected monitor, e.g. changed location of a Device in the GVO Registry) • Check with a GET to the endpoint '/PRRS-service/resource/actionstaken' the context change indeed has produced a reaction.		
Requirements	• PRRS tool installed and accessible in port http 8080. • Define the set of context variables that we can use in the PRRS rule designer. • Define a rule, using the PRRS rule designer in the endpoint '/PRRS-webgui', that complies when the context variable used in this evaluation is changed.		
Metrics and target	Demonstrate that the system is adaptable and can react to context changes on runtime. The results of the actions taken are accessible from the PRRS interface to check them.		
Rank	D	Type	Trial (UC: O2, I1, I2)

ID	AL.SE.4	Name	RE-Mote system update	Category	Security, Automation
Description	Incorporating adaptability to an IoT platform using PRRS and OAP / direct install from console				
Rationale	The OAP resolves the problem of the dynamic actualization of the whole system by automation of software updates and patching. The possibility of updating remote devices without physical intervention is a basic feature to implement this technology.				
Evaluation responsible	ATOS				
Evaluator	Expert				
Evaluation process	**Expert**: • Search the firmware using the tags predefined in the form at the endpoint '/PRRS-webgui'. • Select the concrete firmware to use. • Select the concrete VRD or VRD Federation to update, previously defined in the GVO Manager. • Confirm and launch the update. • Wait for the success response from the target device.				
Requirements	• PRRS tool installed and accessible in port http 8080. • Define the set of tags for identifying the software artefacts. • Integration with the GVO Registry and the RD Deployer.				
Metrics and target	Demonstrate that the system is flexible and scalable because the software of the devices can be updated and modified remotely. The results of the actions taken are accessible from the PRRS interface to check them. A response from the device after the update (firmware installation) ensures the success.				
Rank	M		Type	Trial (UC: O2, I1, I2)	

3 Proof-of-Concept Laboratory experiments

Proof of concept experiments will be conducted in simulations and/or controlled laboratory environments in order to qualitatively and quantitatively assess the performance gains of the protocols and algorithms developed within WP2-WP4, evaluating the performance of the individual system modules in order to identify any issues and to prepare them for the real-world trials in tasks T5.4 and T5.5. These experiments will measure the evaluation criteria of type Lab as indicated in their description in section 2.

3.1 Runtime-, Memory-, Communication-Overhead of Signing and Verifying Message Payload with ECC Standard Signatures in RDs

3.1.1 Purpose of the experiment

The experiment investigates the overheads occurring in devices when the implementation of the ECC based JSON sensor signatures (JSS) is carried out and implemented on RERUM Devices, like Z1 or Re-Mote. These can be applied in almost all UCs. The aim is to validate what the application of ECC signatures on messages has in terms of speed, memory and communication overhead. The whole process can be separated into steps we aim to evaluate them separately, when possible:

- Signing: The generation of the signature could itself potentially be split into steps:
  - (Sign_Step1) POTENTIALLY transform (JSON MINIFY) and encode (BASE64URL) input
  - (Sign_Step2) calculation of a cryptographic hash over encoded input, e.g. SHA 256
  - (Sign_Step3) the actual calculation of the signature value on the digest, and finally
  - (Sign_Step4) the addition of the signature into the structure of the message
- Verification: The verification of a signed message could itself potentially be split into
  - (Vrfy_Step1) parsing the signature from the structure of the message
  - (Vrfy_Step2) POTENTIALLY transform (JSON MINIFY) and de- and en-code (BASE64URL) input
  - (Vrfy_Step3) the actual signature verification value on the digest
- Key-Generation: The generation generates new key material. It is foreseen that this step is not run on the devices itself, or only once at the initial setup. Never the less for completeness, RERUM wants to measure the impact of this step if time permits.
  - (KeyGen_Step1) Generate Key(s)

3.1.2 KPIs

- Crypto-Memory-Consumption-Overhead for ECC Signature on device
- Crypto-Communication-Overhead for ECC Signature on device
- Crypto-Runtime-Overhead for ECC Signature on device

3.1.3 Experimental scenarios

RERUM will choose from available ECC curves and configurations at least ECC based on curve secp256r1, that is the P-256 curve equivalently used in XML Signatures described as http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256 and SHA 256 is planned to be implemented as prototypes in Hardware. Potentially, more secure cryptographic algorithm configurations could be chosen, i.e. SHA 512 or an elliptic curve with points in the size of 512 bit length. The Hardware under test for the resource constrained devices is planned to be either Zolertia Re-MOTE and Zolertia Z1 (if implementation is possible) to run the cryptographic.

To measure the increase, we need a base measurement for reference. This will be the implementation without code for the crypto operations, e.g. the implementation will contain no-operation or libraries are not included. Hence this laboratory experiment will feature two devices: RE-Mote#1 in Figure 4 below is the 'vanilla' device. Vanilla means here that the device contains and especially uses none of the cryptographic features under test. Then device RE-Mote#2 is the device that runs crypto, e.g. signs sensor readings.

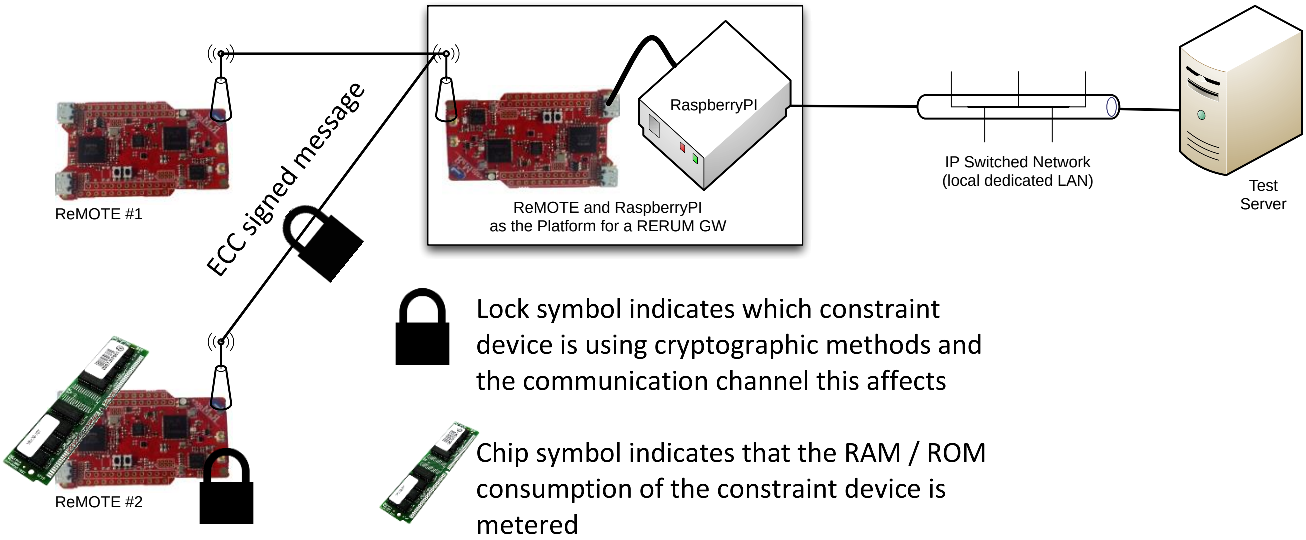

Figure 4 High Level Overview of a potential Experimental Setup: Zolertia's Re-Mote under test for RAM/ROM consumption when testing the application of ECC Signatures (algorithms under test Vrfy and Sign)

The devices under test that this test plans to examine, as referenced in Figure 5, are:

- Zolertia Z1
- Zolertia Re-Mote
- Raspberry Pi (Model B)

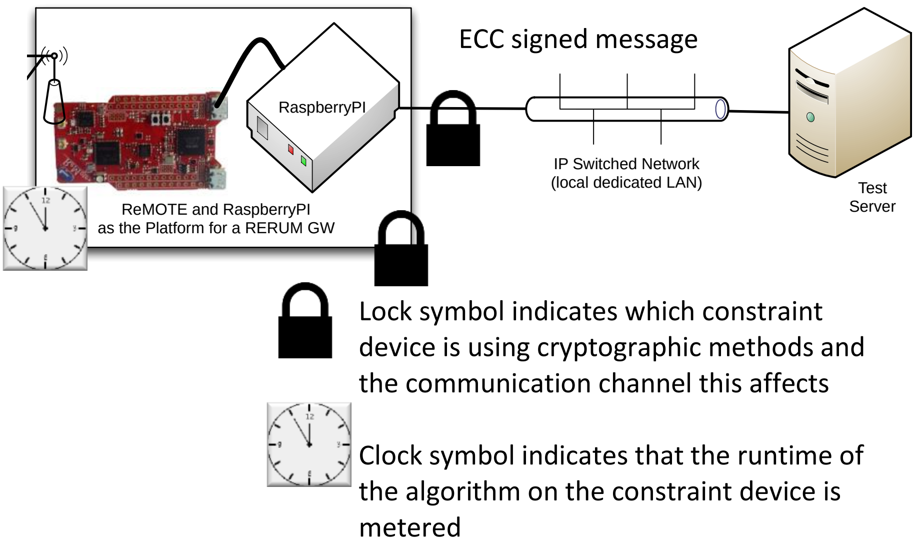

Figure 5 High Level Overview of a potential Experimental Setup: Raspberry PI as Gateway under test for runtime when testing the application of ECC Signatures (algorithms under test Vrfy and Sign)

The following different scenarios will be metered:

3.1.3.1 Experimental scenarios: Runtime-, Memory-, Communication-Overhead of Sign (with sending messages) on Device

In each cycle a counter value is incremented on the device under test and this data is signed and encapsulated into a **signed** message that is sent over the communication channel. The power consumption of this is then compared with the power consumption endured when in each cycle a counter value is incremented on the device under test and encapsulated into a message that **is sent over the communication channel**.

3.1.3.2 Experimental scenarios: Runtime-, Memory-, Communication-Overhead of Verify (with receiving messages) on Device

In each cycle a counter value is incremented on the test server and a signed message is generated, with a key for which the device under test has been deployed with the corresponding verification key. The device under test is **verifying** the message that is **received from the communication channel**. The power consumption of this is compared with the power consumption endured when in each cycle an unsigned counter value is received on the device under test.

3.1.3.3 Experimental scenarios: Runtime-, Memory-, Communication-Overhead of Key Generation (with no communication) on Device

In each cycle a new random key material is generated and stored on the device under test, such that it could be used for further cryptographic operations, e.g. this includes the encoding into some data structure and storage of that in RAM or external Storage.

3.1.4 RERUM architecture functional components involved/tested

Integrity Generator / Verifier

3.1.5 Foreseen experiment risks

None

3.1.6 Timeplan

To be detailed in task 5.2.

3.2 Runtime-, Memory-, Communication-Overhead of Signing, Verifying and Messages with Malleable Signatures in RDs

3.2.1 Purpose of the experiment

The experiment investigates the overheads occurring in devices when the implementation of the Malleable Signature is executed as an implementation on RERUM Devices, like Z1 or RE-Mote. These can be applied in almost all UCs. The aim is to validate what the application of malleable signatures on messages has in terms of speed, memory and communication overhead. The whole process can be separated into steps we aim to evaluate them separately, when possible:

- Signing: The generation of the signature could itself potentially be split into steps:
  - (Sign_Step1) POTENTIALLY transform (JSON MINIFY) and encode (BASE64URL) input
  - (Sign_Step2) calculation of a cryptographic hash over encoded input, e.g. SHA 256
  - (Sign_Step3) the actual calculation of the signature value on the digest, and finally
  - (Sign_Step4) the encoding / addition of the signature into the structure of the message
- Verification: The verification of a signed message could itself potentially be split into steps:
  - (Vrfy_Step1) parsing the signature from the structure of the message
  - (Vrfy_Step2) POTENTIALLY transform (JSON MINIFY) and de- and en-code (BASE64URL) input
  - (Vrfy_Step3) the actual signature verification value on the digest
- Sanitize/Redact: The modification of a message in an authorised way and the re-computation of the signature, such that it still verifies under the signer's verification key could itself potentially be split into steps:
  - (Sanitize/Redact_Step1) parsing the signature and the message from the structure of the message
  - (Sanitize/Redact_Step2) modify the message in an authorised way
  - (Sanitize/Redact_Step2) re-compute the signature on the modified message
  - (Sanitize/Redact_Step2) the encoding / addition of the adapted signature and modified back into the structure of a message
- Key-Generation: The generation generates new key material. It is foreseen that this step is not run on the devices itself, or only once at the initial setup. Never the less for completeness, RERUM wants to measure the impact of this step if time permits.
  - (KeyGen_Step1) Generate Key(s)

3.2.2 KPIs

- Crypto-Memory-Consumption-Overhead for Malleable Signature on device
- Crypto-Communication-Overhead for Malleable Signature on device
- Crypto-Runtime-Overhead for Malleable Signature on device

3.2.3 Experimental scenarios

Same scenarios as with ECC signatures: e.g., 3.1.3.1 for Signing, 3.1.3.2 for Verifying and 3.1.3.3 for Key Generation. Additionally we need to measure the Speed and Storage for the additional algorithms of Sanitize/Redact, which is described as follows in 3.2.3.1.

3.2.3.1 Experimental scenarios: Runtime-, Memory-, Communication-Overhead of Sanitize/Redact (with two way communication) on Device

In each cycle a counter value is incremented on the test server and a malleably signed message is generated, with a sanitizer key (if applicable) for which the device under test has been deployed with the corresponding sanitization key. In each cycle that message is sent over the communication channel to the device under test, which **performs a single sanitization/redaction** and adapts the signature accordingly to the malleable signature scheme under test. This authorised change is then encapsulated into a message with the re-computed signature message that is **sent over the communication channel**. The power consumption of this is then compared with the power consumption endured when in each cycle a message without a signature is just received from the communication channel and the value in it is incremented by one on the device under test and then encapsulated into a message that is sent back over the communication channel.

3.2.4 RERUM architecture functional components involved/tested

Integrity Generator / Verifier

3.2.5 Foreseen experiment risks

None.

3.2.6 Timeplan

To be detailed in task 5.3.

3.3 Energy Efficiency of Malleable Signatures on RDs

3.3.1 Purpose of the experiment

The experiment investigates the power consumption of the implementation of malleable signature schemes. These can be applied in almost all UCs. The aim is to validate what the application of such a malleable signature scheme for messages has in terms of power cost. This experiment will evaluate four different processes as a whole: signing only, sanitization/redaction only, verification only and key generation. Each process includes all its steps and then the communication.

- Signing: The device under test will continuously generate data, sign data, and communicate the signed data.
- Verification: The device under test will continuously receive signed data, and will verify the signature.
- Sanitization/Redaction: The device under test will continuously receive malleable signed data, and will execute a valid sanitization or redaction and update the signature such that it can be sent over the communication channel to still be verified.

As Malleable Signatures might need special keys or cryptographic material, the experiments will try to determine the energy costs of generating new key material:

- Key-Generation: The device under test will continuously generate new key material and store it, such that it could be used for generating signatures.

3.3.2 KPIs

- Crypto-Energy-Consumption of Malleable Signatures on device

3.3.3 Experimental scenarios

For each algorithm that is about to be tested the device under test is given a different task to run continuously. We plan using the powertrace module of Contiki. As a fall back alternative we plan to use measurements of the real batteries power level over time.

The following different scenarios will be metered:

3.3.3.1 Experimental scenarios: Energy Overhead of Sign (with sending messages) on Device

In each cycle a counter value is incremented on the device under test and this data is signed and encapsulated into a malleably **signed** message that is sent over the communication channel. The power consumption of this is compared with the power consumption endured when in each cycle a counter value is incremented on the device under test and encapsulated into a message that **is sent over the communication channel**.

3.3.3.2 Experimental scenarios: Energy Overhead of Verify (with receiving messages) on Device

In each cycle a counter value is incremented on the test server and a malleably signed message is generated, with a key for which the device under test has been deployed with the corresponding verification key. The device under test is **verifying** the message that is **received from the communication channel**. The power consumption of this is compared with the power consumption endured when in each cycle an unsigned counter value is received on the device under test.

3.3.3.3 Experimental scenarios: Energy Overhead of Sanitize/Redact (with two way communication) on Device

In each cycle a counter value is incremented on the test server and a malleably signed message is generated, with a sanitizer key (if applicable) for which the device under test has been deployed with the corresponding sanitization key. In each cycle that message is sent over the communication channel to the device under test, which **performs a single sanitization/redaction** and adapts the signature accordingly to the malleable signature scheme under test. This authorised change is then encapsulated into a message with the re-computed signature message that is **sent over the communication channel**. The power consumption of this is then compared with the power consumption endured when in each cycle a message without a signature is just received from the communication channel and the value in it is incremented by one on the device under test and then encapsulated into a message that is sent back over the communication channel.

3.3.3.4 Experimental scenarios: Energy Overhead of Key Generation (with no communication) on Device

In each cycle a new random key material is generated and stored on the device under test, such that it could be used for further cryptographic operations, e.g. this includes the encoding into some data structure and storage of that in RAM or external Storage. Figure 6 and Figure 7 show the experimental scenarios for the energy overhead consumption for key generation.

The devices under test that this test plans to examine are:

- Zolertia Re-Mote
- Raspberry Pi (Model B)

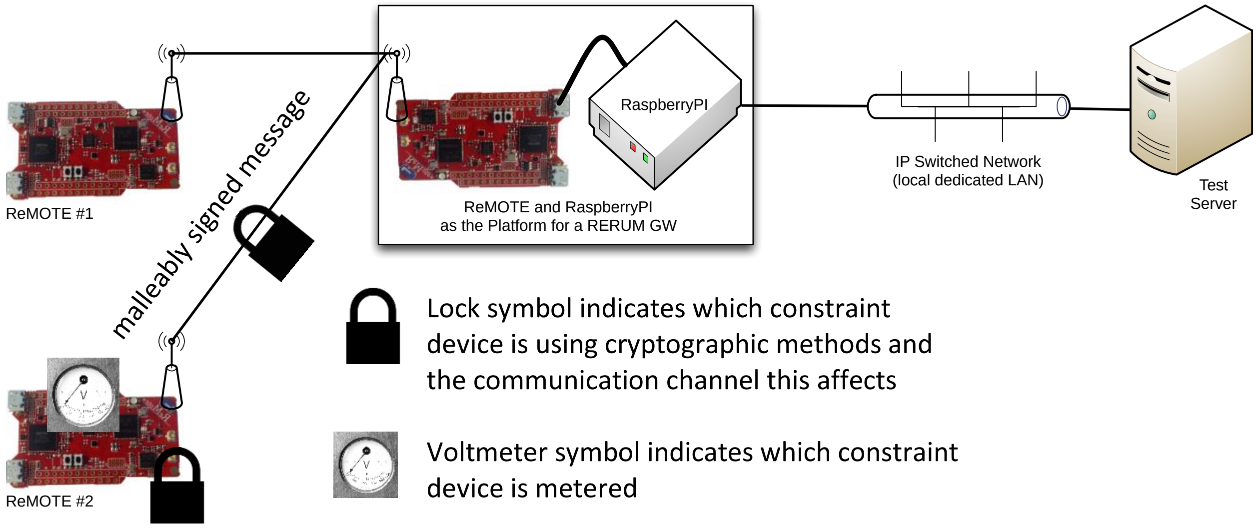

Figure 6 High Level Overview of a potential Experimental Setup: Zolertia's RE-Mote under test for power consumption when testing the application of malleable Signatures (algorithms under test Vrfy and Sign and Sanitize/Redact)

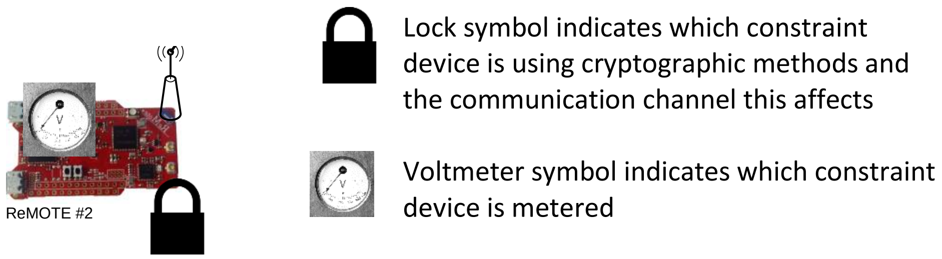

Figure 7 High Level Overview of a potential Experimental Setup: Zolertia's RE-Mote under test for power consumption when generating cryptographic key material (algorithms under test KeyGen)

3.3.4 RERUM architecture functional components involved/tested

Integrity Generator / Verifier

3.3.5 Foreseen experiment risks

None

3.3.6 Timeplan

To be detailed in task 5.3.

3.4 Energy Efficiency of ECC based payload Signatures on RDs

3.4.1 Purpose of the experiment

The experiment investigates the power consumption of the implementation of the ECC based JSON web signatures. These can be applied in almost all UCs. The aim is to validate what the application of ECC signatures on messages has in terms of power cost. This experiment will evaluate two different processes as a whole: signing only and verification only. Each process includes all its steps and then the communication.

- Signing: The device under test will continuously generate data, sign data, and communicate the signed data.
- Verification: The device under test will continuously receive signed data, and will verify the signature.

For completeness we will also try to determine the energy costs of generating new ECC keys:

- Key-Generation: The device under test will continuously generate new key material and store it, such that it could be used for generating signatures.

3.4.2 KPIs

- Crypto-Energy-Consumption of ECC Signature on device

3.4.3 Experimental scenarios

RERUM will choose from available ECC curves and configurations at least ECC based on curve secp256r1, that is the P-256 curve equivalently used in XML Signatures described as http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256 and SHA 256 is planned to be implemented as prototypes in Hardware. The Hardware under test for the resource constrained devices is planned to be either Zolertia RE-Motes or Zolertia Z1 (if implementation is possible) to run the cryptographic.

To measure the increase, we need a base measurement for reference. This will be the implementation without code for the crypto operations, e.g. the implementation will contain no-operation or libraries are not included. Hence this laboratory experiment will feature two devices: RE-Mote#1 in the picture below is the 'vanilla' device. Vanilla means here that the device contains and especially uses none of the cryptographic features under test. Then device RE-Mote#2 is the device that runs crypto, e.g. signs sensor readings.

The detailed scenarios are the same as in the case of malleable signatures, just not the Sanitize/Redact algorithms, i.e. 3.3.3.1 for Sign, and 3.3.3.2 for Verify and 3.3.3.4 for Key Generation. Figure 8 below shows the experimental setup scenario for this test.

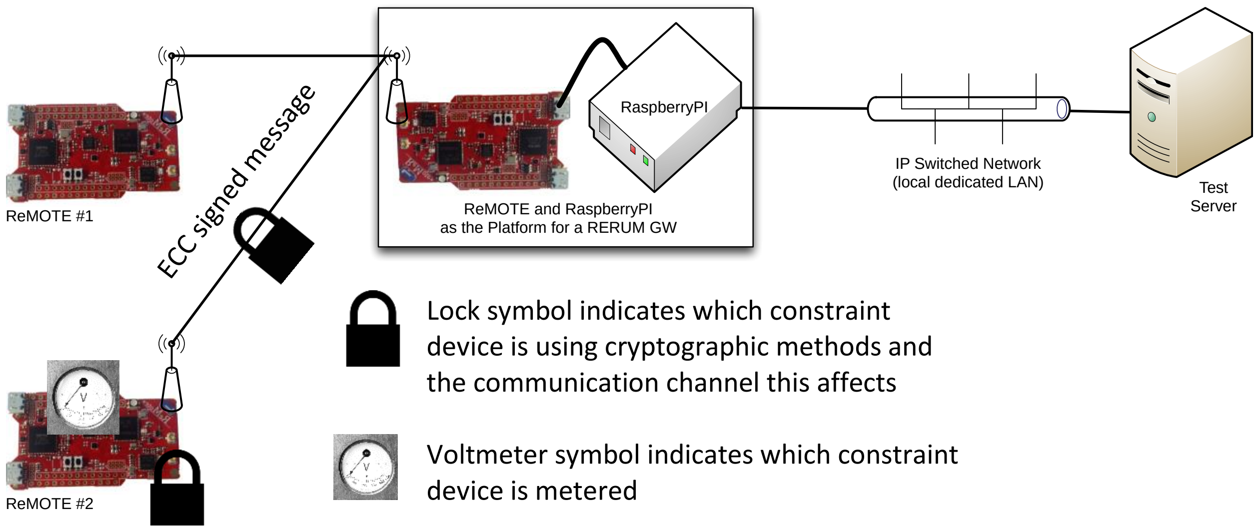

Figure 8 High Level Overview of a potential Experimental Setup: Zolertia's RE-Mote under test for power consumption when testing the application of ECC Signatures (algorithms under test Vrfy and Sign)

3.4.4 RERUM architecture functional components involved/tested

Integrity Generator / Verifier

3.4.5 Foreseen experiment risks

None.

3.4.6 Timeplan

To be detailed in task 5.3.

3.5 RSSI-based CS encryption keys

3.5.1 Purpose of the experiment

The experiment investigates the efficiency of the proposed method for extracting encryption and compression keys that are used for Compressive Sensing in a real-world experiment. This method is described in detail in the deliverable D3.1, where theoretical evaluation is being performed in terms of simulations. The idea here is that this method will be implemented on real hardware and tested in a controlled indoor environment to evaluate its performance. The implementation and testing will be done in laptops because of the current complexity of the method that does not allow us to test it in existing sensor platforms like the Zolertia Z1. However, due to the recent availability of the new sensor platform from Zolertia that is designed according to the RERUM requirements, the implementation of the RSSI key extraction mechanism on the RE-Mote will be studied in the next months.

The experiment requires the implementation of three nodes, two of them are legitimate and one is the malicious node. The legitimate nodes are trying to agree on a common key to use it for CS encryption and encrypt the measurements that they exchange. The malicious node also runs the same algorithm with the legitimate nodes and tries to identify the key of the legitimate nodes. The goal of the experiment is to show that if the malicious node is further than a specific distance from the legitimate nodes, it has a very high reconstruction error, which means that its encryption key differs significantly compared with the key of the legitimate nodes.

So, in this experiment we will test the efficiency of the method both in terms of reconstruction error for the legitimate nodes and for the malicious node.

3.5.2 KPIs

The KPIs that will be measured within this experiment are the following:

- Time required to agree on a common CS key (actual time in seconds and relative time in terms of number of exchanged packets required)
- Legitimate nodes' reconstruction error
- Malicious node reconstruction error
- Bit mismatch rate between the keys derived by the legitimate nodes
- Bit mismatch rate between the keys derived by the malicious node and the legitimate nodes

3.5.3 Experimental scenarios

This experiment will be run on a specific topology that is shown in Figure 9. In this topology we have three devices that could be either laptops or RE-Motes. No other devices are required for this experiment. All devices are wirelessly interconnected (the wireless technology is not important, either IEEE 802.11 or IEEE 802.15.4 can be used). All devices are running the exact same program for extracting CS keys using RSSI measurements and then use this key for decrypting/decompressing the measurements that they gather.

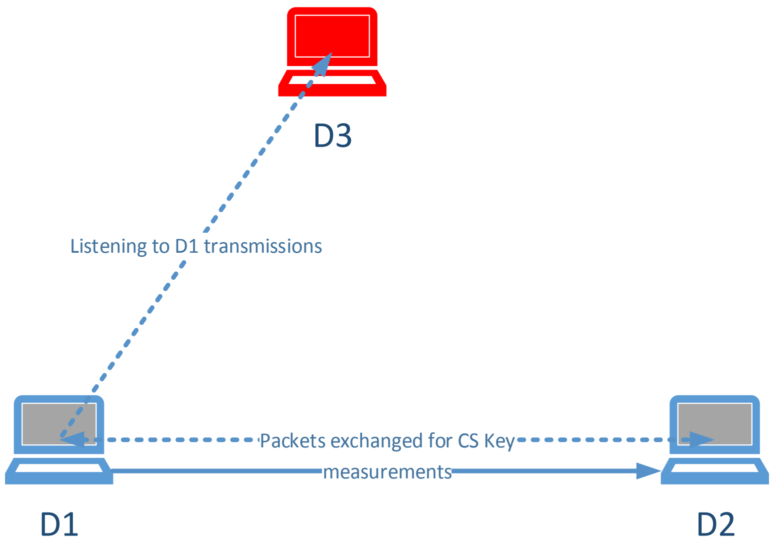

Figure 9 Topology of the RSSI-based CS key extraction experiment

One of the legitimate devices plays the role of the sensor that gathers measurements, while the other legitimate device receives the measurements and decrypts them. The malicious node plays the role of a passive listener that receives the measurements and tries to decrypt them using the key that he has derived.

So, the devices in this experiment are the following:

- D1: legitimate device – gathers measurements and wants to transmit them to D2.
- D2: legitimate device – receives the measurements from D1
- D3: malicious device – receives the measurements from D1 and wants to decrypt them.

And the process followed in the experiment scenario is:

- D1 exchanges packets with D2.
- D3 receives the packets sent by D1.

- D1 and D2 derive their CS keys using the method and identify the common key.
- D3 derives its CS key.
- These keys are compared with each other in order to calculate the bit mismatch error between:
    - D1_key and D2_key
    - D3_key and D1_key
- D1 encrypts the measurements and sends them to D2. The measurements are also stored in order to be used for comparing them with those of D2 and D3 to calculate the reconstruction errors.
- D2 and D3 receive and decrypt the measurements.
- The reconstruction error of the measurements received by D2 and D3 are calculated (comparing the decrypted measurements with the originals) and the reconstruction errors are compared with each other.

This scenario will be repeated for different distances between the devices in order to calculate how the distance affects the difference in the reconstruction errors.

3.5.4 RERUM architecture functional components involved/tested

- Data encrypter/decrypter

3.5.5 Foreseen experiment risks

There is a risk inherent in this experiment and is related with the effect of the multipath phenomena on the RSSI, so indoor experiments may not have good results. In this case the experiments will be repeated in more indoor areas.

3.5.6 Timeplan

Indicative timeplan for this experiment:

- Implementation of the programs for deriving CS keys: until June 2015
- First set of experiments run indoor: until August 2015.
- Evaluation of the results: September 2015

3.6 Adaptive CS-based data gathering

3.6.1 Purpose of the experiment

The goal of this experiment is to evaluate the performance and the efficiency of the adaptive CS-based data gathering mechanism that has been developed within RERUM. This mechanism aims to provide a secure and energy-efficient way of gathering sensing measurements from constrained IoT devices that can provide services with different Quality of Service (QoS) requirements. This mechanism will be described in detail in deliverable D4.2 (due end of August 2015), but is also published in [1]. The basic idea is that we utilize the Compressive Sensing technique in order to compress blocks of measurements and transmit much less packets than if we did not compress/encrypt the measurements. Thus, we save a significant amount of transmission energy with only a very small fraction of additional energy spent in CPU. Furthermore, due to the inherent security features of the CS technique, the transmitted measurements will also be encrypted.

This experiment will use real devices and will run on both Zolertia Z1s and RE-Motes. A comparison of the performance of the mechanism when it is run on RE-Motes compared with Z1s will also be done.

The experiment may include several devices, however a minimum of one IoT device is required for the experiment and then a target device that does the decryption of the measurements and could be

(i) the gateway, (ii) the RERUM Middleware or (iii) an application server. The target device needs to know the QoS requirements of the service to be provided by the device in order to identify the target compression rate.

3.6.2 KPIs

The KPIs that will be measured within this experiment are the following:

- Reconstruction error at the receiver
- Percentage of time the reconstruction error stays above the threshold defined by the QoS of the provided service class
- Energy consumption of this technique compared with the energy consumed when transmitted uncompressed measurements
- Time required to detect changes in the signal sparsity and adapting to a new compression rate
- False alarms/misdetections in sparsity changes
- Communication overhead (increased signalling) for adapting to the sparsity changes

3.6.3 Experimental scenarios

This experiment will be run on a specific topology that is shown in Figure 10. In this topology we have three devices, one playing the role of the client that gathers, compresses and transmits the measurements, an intermediate device playing the role of a router and another device playing the role of the receiver that receives the measurements and decompresses them. The client (Z1 or RE-Mote) will utilize a standard IEEE 802.15.4 wireless interface. The intermediate router can also be discarded if the receiver device has an IEEE 802.15.4 interface. However, in the experiments the receiver will be a standard laptop or a PC, so there is the need for the intermediate router to route the packets from the IEEE 802.15.4 interface to the standard IEEE 802.11 interface to transmit the packets to the laptop/PC. This is a bare minimum of devices that are required to execute this experiment. However, other clients may also be included if needed, but each one will be separately handled by the receiver. We assume that the receiver is powerful enough to handle multiple different clients simultaneously, so no scalability evaluation is required at this experiment.

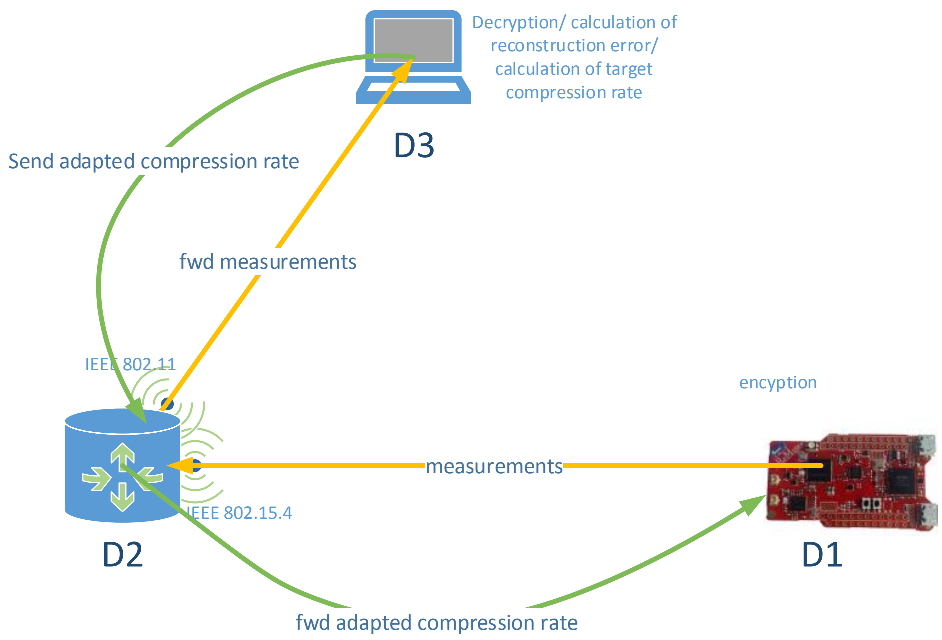

Figure 10 Topology of adaptive CS data gathering experiment

So, the devices in this experiment are the following:

- D1: client device – gathers measurements, encrypts them and transmits them to D3 (through D2).
- D2: router device – receives the measurements from D1 through the IEEE 802.15.4 interface and routes them to D3 through the IEEE 802.11 interface.
- D3: server device – receives the measurements from D1, and decrypts them.

For the sake of simplicity of the experiment, the RERUM Middleware is avoided.

For the experiments we envisage the scenarios described below.

Scenario1

This is a simplistic scenario that aims to evaluate the reconstruction error at the receiver and the energy consumption of the client device and has the following process:

- D1 gathers the measurements, encrypts them and sends them to D3.
- D1 also measures the energy consumed for transmitting a specific number of measurements.
- D3 receives the measurements, decrypts them and evaluates the reconstruction error.
- D1 repeats the same process for measurements that are not compressed in order to measure the energy consumption for a full set of measurements.

This scenario will be repeated for different compression rates, ranging from 20% to 80% in order to see the performance of the mechanism and the energy saved by using the proposed CS method.

Scenario2

This is a more advanced scenario that aims to evaluate the efficiency of the adaptive CS technique. In this scenario, the receiver will evaluate the reconstruction error and compare it against a threshold set by the QoS of the service class that is provided by the client. Then, if the error is higher, the receiver will calculate the new compression rate that is required to have an error within the QoS limits and will send the new compression rate back to the client device in order to adjust the compression rate. This process will be run on the RE-Mote as a client device which is quite powerful in terms of memory to handle this process. A simplistic implementation on the Z1 will also be tested, but due to the very strict hardware limitations in terms of memory it is not ensured that the process will run efficiently.

The process of the experiment is the following (the comparison of the energy consumption is not performed in this scenario because the results will not differ compared with those of the previous scenario):

- D1 gathers the measurements, encrypts them and sends them to D3.
- D3 receives the measurements, decrypts them and evaluates the reconstruction error.
- D3 compares the error against the threshold set by the QoS of the service class provided by D1.
- If the error is higher than the threshold, D3 calculates the target compression rate for adjusting the reconstruction error.
- On the contrary, if the error is very much lower than the threshold (which means that D1 does not do the maximum compression allowed consuming more energy) then D3 also calculates the optimum compression rate in this case.
- If D3 cannot calculate directly the optimum compression rate, it may ask D1 for additional measurements.
- D3 sends the target optimum compression rate back to D1.

- D1 receives the optimum compression rate and adjusts the compression matrix accordingly for the next set of measurements.
- The number of additional packets with measurements required by D3 to calculate the new compression rate will be measured by D3 to assess the communication cost incurred by the mechanism.

This scenario will be repeated for different service classes with different reconstruction error thresholds to see the performance of the mechanism and the speed to calculate and adapt to the new compression rate.

3.6.4 RERUM architecture functional components involved/tested

- Data encrypter/decrypter
- RD adapter
- Module for data gathering (Resource manager in the RD adapter)
- Energy efficiency non functional requirement

3.6.5 Foreseen experiment risks

Complexity of the mechanism and high memory requirement may disallow the implementation on the Z1.

3.6.6 Timeplan

Indicative timeplan for this experiment:

- Implementation of the resource manager for the device: until June 2015
- First set of experiments run indoor: until July 2015.
- Evaluation of the results: August-September 2015

3.7 Sensor self-monitoring

3.7.1 Purpose of the experiment

The goal of the experiment is to evaluate the performance of the self-monitoring mechanism developed within RERUM. This mechanism is presented in detail in RERUM Deliverable D3.1. Its objective is to gather both network and device statistics from the RERUM Devices (RDs) in an energy efficient and effective way. These statistics will be sent to the centralized RERUM MW in order to be utilized by the Resource Monitor and the Alert Processor to identify possible problems with the network mechanisms (i.e. channel assignment, routing) or with the devices themselves (i.e. device is shut down) and try to resolve the issue. In this respect, the devices gather both types of statistics and periodically sends them to the MW.

This experiment aims to implement this mechanism in real devices, using both RE-Mote and Z1s. The mechanisms to gather the statistics will be implemented on Contiki and installed on the devices. The experiment focuses only on gathering and transmitting these measurements/statistics and not on the server-side exploitation of these statistics. Thus the implementations of the Resource Monitor and the Alert Processor are out of the scope of this experiment.

The module that gets the statistics and transmits them to the MW (or to the server) is implemented as an IoT Resource on the RDs and a Service is exposing this Resource. On the MW side, we have a specific application that accesses this Service and presents the results on a graph.

3.7.2 KPIs

The KPIs that will be measured within this experiment are the following:

- Both network statistics and device statistics will be measured.
- The period of transmitting the statistics and its effect on the energy consumption of the devices will be evaluated.
- The communication overhead (increased signalling) for transmitting the statistics will be calculated.
- The period of transmitting the statistics and its effect on identifying network/device errors will be calculated.

3.7.3 Experimental scenarios

This experiment will be run on a topology like the one shown in the previous **Figure 10**, with the client (D1) being a Z1 or a RE-Mote, D2 being still the router and D3 playing the role of both the RERUM MW and the application server. This is a bare minimum of devices that are required to execute this experiment. However, other clients may also be included if needed, but each one will be separately handled by the MW (D3). We assume that both the MW and the router are powerful enough to handle multiple different clients simultaneously, so no scalability evaluation is required at this experiment.

So, the devices in this experiment are the following:

- D1: RERUM device that needs to be self-monitored. It has a Resource for "self-monitoring" which is exposed by a Service. Listens for service requests that are sent by the MW. It gathers both network and device statistics, encrypts them and transmits them to D3 (through D2).
- D2: router device – receives the statistics from D1 through the IEEE 802.15.4 interface and routes them to D3 through the IEEE 802.11 interface.
- D3: MW and application server – listens for application requests, sends service requests to D1, receives the statistics from D1, and displays them.

For the experiments we envisage the scenario described below (we assume that the registration of RD D1 on the MW has already been done before starting this process):

- An administrator creates an application in D3 to request the monitoring statistics of D1.
- D3 translates the application to a service requests and invokes the "self-monitoring" Service of D1, by sending an http/coap request to the device.
- D1 gets the service request and accesses the "self-monitoring" Resource that gathers (periodically) both the network and device statistics. The period is set by the service request according to a parameter set by the administrator when he requests the application.
- D1 sends periodically the statistics to D3.
- D3 gathers the statistics and displays them.
- D1 measures the energy consumed by both the CPU that gathers the statistics and the Radio interface that transmits the measurements.
- D3 measures the network load due to the network statistics that are exchanged.

This scenario will be repeated for different periods of monitoring and with more than one RDs. The scenario will be run for both the Z1 and the RE-Mote. The energy consumed for self-monitoring by both Z1 and RE-Mote will be calculated and compared with each other.

3.7.4 RERUM architecture functional components involved/tested

- RD adapter
    - Resource Manager
    - RERUM Services wrapper
- Network monitoring

3.7.5 Foreseen experiment risks

No risks are foreseen in this experiment. The mechanisms are very lightweight and will run flawlessly in both Z1 and RE-Mote.

3.7.6 Timeplan

Indicative timeplan for this experiment:

- Implementation of the Network Monitoring module for the Z1: until April 2015
- First set of experiments run for the Z1s: until May 2015.
- Implementation of the Network Monitoring module for the RE-Mote: until May 2015
- First set of experiments run for the RE-Mote: until June 2015.
- Evaluation of the results: July 2015

3.8 Lightweight spectrum sensing and spectrum assignment framework

3.8.1 Purpose of the experiment

The goal of this experiment is to evaluate in a controlled laboratory environment the efficiency of the lightweight spectrum sensing and spectrum assignment frameworks. The target evaluated modules are those for gathering spectrum occupancy measurements and modelling the spectrum occupancy, as well as the module for spectrum assignment. These mechanisms are explained in detail in deliverable D4.1.

The purpose of the spectrum sensing module is to allow the Cognitive Radio-based RDs to be able to gather spectrum occupancy statistics in an energy efficient way and then extract models of the spectrum occupancy of specific bands. This will minimize the energy consumed by the RDs for sensing the available spectrum bands, by extracting an optimum period for sensing each band and avoid sensing the bands very frequently (process that consumes a lot of energy).

The purpose of the spectrum assignment module is to allow the Cognitive Radio-based RDs to select the most appropriate and suitable spectrum band for meeting the transmission requirements of the service class(es) it provides. A basic target in this spectrum assignment mechanism is to meet the QoS requirements of the service class and to select the most suitable spectrum, in terms of optimal central frequency and band width for this transmission and all these with an objective to consume a minimum amount of energy.

For both experiment scenarios due to hardware requirements and the fact that Cognitive Radio mechanisms require running on top of Software-Defined-Radio (SDR) devices, this mechanism can’t be implemented on existing IoT platforms like Z1 or RE-Mote. In this respect, standard SDR devices will be utilized in this experiment in order to evaluate the performance of the proposed mechanism.

3.8.2 KPIs

The KPIs that will be measured within this set of experiments are the following:

- Speed of convergence to the optimum period for spectrum sensing.
- Energy consumed for sensing until the convergence is reached.
- Energy consumed for sensing using the optimum period.
- False positives and false negatives when sensing the spectrum after converging to the optimum period.
- Comparison of the energy consumed in the overall process compared with a standard spectrum sensing mechanism.

- Scalability of the mechanism when the number of the available spectrum bands that the RD senses increases.
- Power consumption for transmitting at the selected frequency/bandwidth.
- Percentage of service requests accepted and served with the required QoS.

3.8.3 Experimental scenarios

This experiment requires only one device that plays the role of the RD, having installed the mechanism for lightweight spectrum sensing. Then, this RD will sense the spectrum at specific spectrum bands, in order to identify the optimum period for sensing. However, since this experiment will be executed at indoor environments and the RD will select to sense spectrum fragments at the TV-bands (below 900MHz) it will be difficult to sense accurately real transmissions and to know their transmission model in order to evaluate if the spectrum occupancy model extracted by the RD is accurate. Thus, for the sake of the experiment and to be able to make a proper evaluation of the results, another SDR device will be used to play the role of a licensed user that transmits according to pre-defined models at a specific spectrum band.

The scenarios run in the experiment are described below.

Scenario 1 (spectrum occupancy measurements)

- The RD is an SDR-based device (laptop with an SDR PCI express card) capable of sensing a wide spectrum band.
- The licensed user is another SDR device that will have installed a specific transmission model.
- The RD will start sensing the spectrum band that is only used by the licensed user according to the spectrum sensing mechanism.
- After an amount of time the RD will have converged to the optimum sensing period and will have extracted a model of the transmission of the licensed user (depending on the characteristics of the model)
- The speed of convergence to the optimum period in terms of time (number of timeslots) will be assessed.
- The energy consumed until the convergence will be measured together with the energy consumed for each period of sensing.

This experiment will be run for different timeslots and for different transmission models of the licensed user. The goal is to evaluate the speed of convergence and the energy consumption for each set of experiments.

Scenario 2 (lightweight spectrum assignment)

- The RD is an SDR-based device (laptop with an SDR PCI express card) capable of accessing a specific band width of the spectrum. The RD has a set of service classes with specific requirements in terms of QoS (specifically bandwidth).
- There are several licensed users (emulated by another SDR device) that will transmit on different/adjacent spectrum bands.
- The RD will start run the mechanism for selecting the spectrum frequency and the band width for meeting the service requirements.
- A third device will play the role of the gateway that will have the server-side application for the spectrum assignment that will take out all the complexity from the RD.
- The energy consumed for transmitting at the specific band will be measured by the device.

This experiment will be run for different service classes of the device and different number of licensed users and band widths.

3.8.4 RERUM architecture functional components involved/tested

- CR-agent (spectrum sensing module)

- CR-agent (spectrum assignment module)

3.8.5 Foreseen experiment risks

For the spectrum occupancy measurements framework there is an inherent risk in this experiment that the proposed model takes a lot of time to converge to the optimum sensing period and this depends on the timeslot that is selected, because the convergence time is directly proportional to the timeslot. Thus, at the beginning a short timeslot will be selected to avoid unneeded delays in the running of the experiment.

For the lightweight spectrum assignment, depending on the occupancy of the available spectrum bands, the problem of finding suitable bands may be infeasible, but the setup of the experiment will be such that a solution is always available.

3.8.6 Timeplan

Indicative timeplan for this experiment:

- Implementation of the licensed user that will emulate different transmissions: starting on May until June 2015
- Implementation of the CR-agent on the SDR device: until August 2015
- First set of experiments: until October 2015
- Evaluation of the results and re-run: until December 2015

3.9 CR-based gateway

3.9.1 Purpose of the experiment

The goal of this experiment is to evaluate the efficiency of the implementation of the CR-based gateway. This implementation of the CR gateway is described briefly in D4.1. It has only one SDR card on board and by using SDR technology it is able to emulate transmissions of two different networking technologies, namely IEEE 802.15.4 and IEEE 802.11 and integrate them at the same time serving multiple users of both technologies. The gateway is very important in IoT scenarios due to the fact that it is controlled completely by software and can be utilized to serve even more technologies by installing the required software. The antennas used span from few MHz up to 6GHz so they can be used for many other transmission technologies. Thus, in future IoT scenarios with RDs that apply Dynamic Spectrum Access mechanisms, this type of a gateway will be mandatory to ensure an efficient interconnection of RDs with diverse and heterogeneous types of traffic and different technologies.

3.9.2 KPIs

The KPIs that will be measured within this experiment are the following:

- CPU and RAM utilization for each of the networking technologies
- Power consumption
- Spectrum utilization
- Scalability of the gateway cannot be evaluated in experiments due to the limited number of SDR devices that we have.

3.9.3 Experimental scenarios

This experiment will be run on a topology like the one shown in Figure 11 below. There are two RDs, one being connected with a IEEE 802.15.4 interface (Z1 or RE-Mote) and another one connected with a standard IEEE 802.11 interface (laptop or smartphone). These devices are connected with the SDR-based gateway that also has an Ethernet connection with a server that runs the RERUM MW. The goal of the experiment scenario is to show that both devices can send their measurements to the MW through the SDR-based gateway in an efficient and timely way.

So, the devices in this experiment are the following:

- D1: RERUM device connected through IEEE 802.15.4 that gets sensor reading and transmits them to the MW.
- D2: RERUM device connected through IEEE 802.11 that gets sensor readings and transmits them to the MW through the GW.
- GW: this is the SDR-based gateway, implemented on a standard mini-PC with an SDR card connected to a PCI express slot that emulates both network interfaces for IEEE 802.11 and IEEE 802.15.4. The GW is connected to the MW through an Ethernet interface.
- MW: this is a device that plays the role of both the MW and the application server. It sends service requests to the device and receives their measurements, displaying the results.

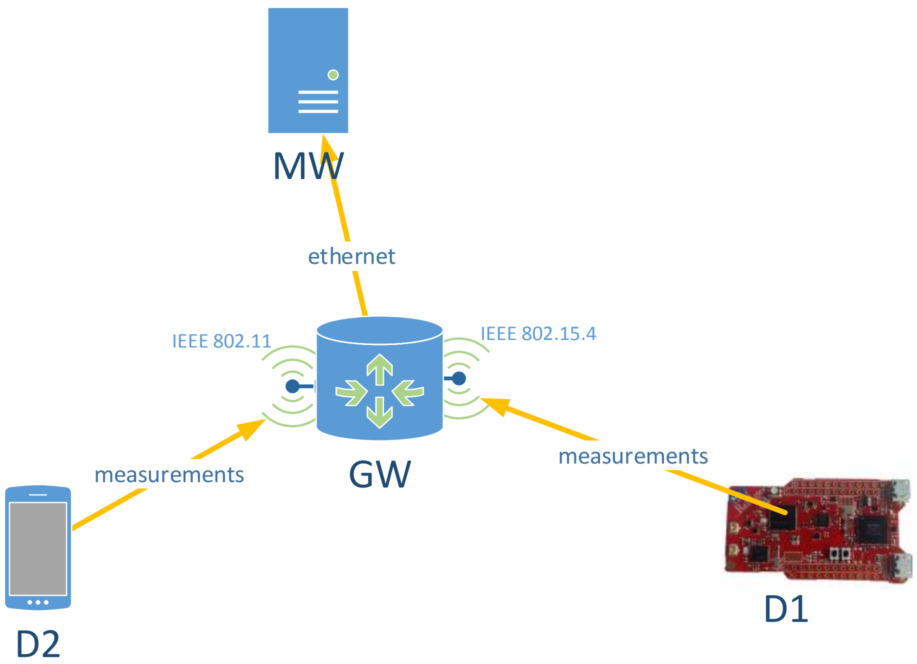

Figure 11 Topology of the SDR-based gateway experiment

For the experiments we envisage the scenario described below (we assume that the registration of D1 and D2 on the MW have already been done before starting this process):

- An administrator creates an application in the MW to request measurements from the two devices (D1 and D2).
- The MW translates the application to service requests and invokes the Services on the devices.
- The GW receives the packets from the Ethernet interface and routes them accordingly to the packets, by appropriately scheduling them and sending them to the correct (virtual) network interfaces for each device.
- The devices get the service requests and accesses the respective Resources, gathering the sensor measurements and sending them back to the MW through the GW.

The experiment will be repeated for different amounts of traffic from the devices in order to assess the performance of the gateway in terms of CPU utilization, memory usage, power consumption and spectrum utilization.

3.9.4 RERUM architecture functional components involved/tested

- Communication manager/routing
- Communication manager/protocol translation
- Communication manager/interface selection
- Communication manager/scheduling

3.9.5 Foreseen experiment risks

The foreseen experiment risks depend on the use of the SDR devices and their efficiency, because existing SDR cards are not working perfectly.

3.9.6 Timeplan

Indicative timeplan for this experiment:

- Implementation of the various modules of the gateway for emulating IEEE 802.11 and IEEE 802.15.4: end of March
- First set of experiments: until June 2015
- Evaluation of results: until July 2015

3.10 Android-based RDs applications & services stability and accuracy

3.10.1 Purpose of the experiment

These experiment target to verify that the android application & servers developed for the participatory sensing in the UC-O1 perform well with respect to unexpected system crashes and the human user. The experiments described herein will be conducted interleaved with the development process to evaluate a set of KPIs.

3.10.2 KPIs

- CPU Load of mobile device
- App. & Server Uptime & Crash Frequency

3.10.3 Experimental scenarios

We have designed four scenarios for experiments to assess the performance and test the developed components. For the first two android app tests we will follow the guidelines and test sheets of the *AQuA (App Quality Alliance) Testing Criteria for Android Applications*[1]. For the latter two we will conduct experiments with fabricated data first on simulation and then on the actually deployed server. Note that since the traffic estimation application itself falls outside of the RERUM scope, there is no associated RERUM KPI for the accuracy of estimator. The aim is to compare whether the RERUM functionalities hinder the performance of an off-the shelf estimator.

3.10.3.1 Android app CPU load measurements

Using standard Android SDK functionalities (Dev Tools App) over the android emulator Android Studio we will initially test the CPU load of the application before passing it on the device. Still, this

[1] **http://www.appqualityalliance.org/files/AQuA_testing_criteria_for_Android_for_v1.4%20final%207_feb_2013.pdf**

will be tested even on the real hardware, to validate the there are no significantly long CPU usage times on the finalized implementation.

3.10.3.2 Android app stability tests

A brief lab campaign will be conducted where the application will be stressed by (i) being overloaded with high frequencies of sensory data transmission and (ii) large numbers of multiple requests.

3.10.3.3 Traffic estimator server stability tests

These experiment scenarios target to verify the application server for the traffic estimation in the UC-O1 performs well. Doing so will require to (i) examine the stability in time under normal operating conditions, (ii) stress the estimator with high loads of input from participatory devices.

3.10.3.4 Traffic estimator accuracy

Note that since the traffic estimation application itself falls outside of the RERUM scope, there is no associated RERUM KPI for the accuracy of estimator. The aim is to compare whether the RERUM functionalities hinder the performance of an off-the shelf estimator.

3.10.4 RERUM architecture functional components involved/tested

Communication and Network Manager, Configuration & Monitoring Manager

3.10.5 Foreseen experiment risks

N/A.

3.10.6 Timeplan

Indicative timeplan for this experiment:

To be detailed in task 5.3.

3.11 Energy Efficiency of Android-based RDs

3.11.1 Purpose of the experiment

The experiment investigates the power consumption of the implementation of the android application for participatory sensing in the UC-O1. The aim is to validate that the application performs effective sensing of the required traffic primitives, at no substantial power cost.

3.11.2 KPIs

- Power Consumption rates (Android)

3.11.3 Experimental scenarios

3.11.3.1 Long term power consumption versus the load of requested data

This scenario aims at investigating the power cost of the privacy enhancing mechanisms implemented on the app. Specifically we will investigate how the frequency with which the app collects and transmits data affects the power consumption. The aim is to identify potential components that are performing poorly and enhance the implementation. In this scenario, also different techniques for mobility detection and alternative positioning, e.g. WiFi or cellular positioning, will be evaluated.

3.11.3.2 Power consumption of CS processes

This scenario aims at investigating the power cost of the CS implementation on the app. To this end we will compare the power cost of collecting and transmitting traffic primitives with and without the CS mechanism enabled. Trade-offs arising on the compression level / compression matrix size will be investigated against their power costs.

3.11.4 RERUM architecture functional components involved/tested

Data Manager

3.11.5 Foreseen experiment risks

N/A.

3.11.6 Timeplan

Indicative timeplan for this experiment:

To be detailed in task 5.3.

3.12 Android pilot devices measurements precision

3.12.1 Purpose of the experiment

The purpose of the experiment is to evaluate different devices and their capabilities for possibility of using Android-based participatory sensing. Specifically the inputs regarding key sensors for location positioning will be performed. Furthermore, it can act as a reference for the applications server: which given a device model it can infer trust metrics on the collected values.

3.12.2 KPIs

- Measurement precision.

3.12.3 Experimental scenario

3.12.3.1 Location Precision

In this set of scenarios the measurements collection application will be run to test the device GPS in terms of (1) time-to-first-fix and (2) variability/precision. The experiments carried out will be done with at least 3 different candidate devices for the pilot trial and performed in different location settings: in city wide road (squares), in city narrows (single lane – tall buildings), suburban environment and both within a vehicle and out of. Each set of measurements will be performed with a set of fixed device orientations.

3.12.3.2 Signal Strength Precision

In this set of scenarios the measurements collection application will be run to test the device signal strength measurement precision at different locations as with the location precision. In both experiments the output will be a dataset that will be used to identify the most appropriate device for the pilot trials as well as evaluate the effect of errors on different types of sensors for the traffic estimation application.

3.12.4 RERUM architecture functional components involved/tested

Data Manager

3.12.5 Foreseen experiment risks

Stability of the SNR API for different android versions and phones may limit the available number of android devices which can be utilized in the participatory sensing for the trials.

3.12.6 Timeplan

Indicative timeplan for this experiment:

To be detailed in task 5.3.

3.13 6LoWPAN Multicast

3.13.1 Purpose of the experiment

The purpose of these experiments will be to demonstrate how M/W functions can leverage IPv6 multicast in order to improve network performance and decrease energy consumption, ultimately increasing the lifetime of a smart object deployment.

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.

3.13.2 KPIs

The KPIs that will be measured within this experiment are the following:

- **Suitability for embedded devices**: by measuring code size and RAM footprint. Targets for the RE-Mote platform: <3 KB and <3 KB increase respectively for modules required for Multicast functionality, compared to builds without multicast support.
- **Reliability**: by measuring packet loss / packet delivery ratio. Target: This metric is highly-sensitive to traffic rate, network topology, node configuration etc. Therefore, it will be evaluated through comparisons with current state-of-the-art.
- **Network Delay**: Target <1 sec per network hop

3.13.3 Experimental scenarios

6LoWPAN multicast functionality will be tested for two algorithms:

- The BMFA algorithm developed by RERUM and
- The MPL algorithm, which is the current recommendation of the IETF
- No multicast support, whereby each transmission of a datagram to multiple nodes is achieved by the transmission of multiple unicast datagrams.

The aim will be to compare the performance of the two algorithms under different traffic scenarios and network conditions and to evaluate the usefulness of multicast support in comparison to deployments with lack thereof.

3.13.3.1 Suitability for embedded devices - Code size and RAM footprint

Code footprint and RAM requirements will be measured at compile-time. This is achieved by building a firmware image and by subsequently running the toolchain's `-size` command on object files. For example:

```
$ arm-none-eabi-size obj_remote/rpl.o
   text       data        bss        dec        hex    filename
    516          0          1        517        205  obj_remote/rpl.o
```

Figure 12 Code size and RAM footprint for a single code module

The module `rpl.o` is Contiki's core of the implementation of the RPL protocol. This output (Figure 12) provides the following information about this code module:

- Code footprint, including program memory and constant (`const`) expressions (`text`): 516 bytes
- Variables initialized at compile time (`data`): 0 bytes
- Space reserved for variables which are not initialized at compile time (`bss`): 1 byte

The same command can be executed on the entire binary image, for example:

```
$ arm-none-eabi-size mqtt-demo.elf
   text       data        bss        dec        hex    filename
  53492        474      15407      69373      10efd    mqtt-demo.elf
```

Figure 13 Code size and RAM footprint for an entire firmware image

The output of Figure 13 provides the following information about the entire firmware:

- Code footprint, including program memory and constant (`const`) expressions (`text`): 53492 bytes
- Variables initialized at compile time (`data`): 474 bytes
- Space reserved for variables which are not initialized at compile time (`bss`): 15407 bytes

This information will vary for different configurations of a build. We shall calculate this metric for both multicast algorithms as well as for images without multicast support.

3.13.3.2 Lab Experiments – Reliability Measurements and Network Delay.

In order to evaluate the remaining KPIs mentioned above, we will perform the following steps:

- Write a simple application, to be executed on the gateway, which will be able to send multicast traffic to the 6LoWPAN. This application will be able to send datagrams of different (constant or variable) sizes at varying data rates and inter-datagram intervals. It will also be able to collect results at the end of each experiment and to save them in log files suitable for subsequent processing.
- Build firmware images (subscriber firmware) for an RD that needs to receive UDP application layer traffic. We will build three such images:
    - One with BMFA support
    - One with MPL support
    - One without multicast support

  For the former two images, the RD will subscribe to a multicast group.

- Build a second batch of firmware images (router firmware) for an RD that does not need to subscribe to a multicast group. Again, we shall build three such images.
    - One with BMFA support
    - One with MPL support
    - One without multicast support

We will then program a number of nodes (Zolertia Re-Mote devices) with a subscriber firmware and a number of nodes with router firmware. Subsequently, we will deploy those nodes in an indoor lab environment. Figure 14 presents an indicative resulting topology. We will then execute the aforementioned application on the gateway to generate multicast traffic. We will perform experiments under multiple permutations, by modifying the following parameters for each run:

- **Datagram size**: We will test performance under different application layer payloads to determine how the mechanism performs under datagrams of different sizes.
- **Inter-datagram interval (constant of variable)**: In some experiments the time between two consecutive datagram transmissions will be fixed (e.g. 5 seconds). We will test the performance of the algorithms using a variety of intervals, ranging from very short (e.g. 250ms) to some considerably longer value (e.g. 30 secs). We will also test performance a under varying interval (e.g. random interval in [250ms , 30sec]).

Each run will be repeated multiple times to increase the reliability of measurements and to factor out measurement deviations caused by transient phenomena.

We will then modify one of the aforementioned two parameters and repeat the measurements. By changing one of the aforementioned parameters, we will achieve two traffic types: Some runs will use Constant Bit Rate (CBR) traffic and some will use Variable Bit Rate (VBR).

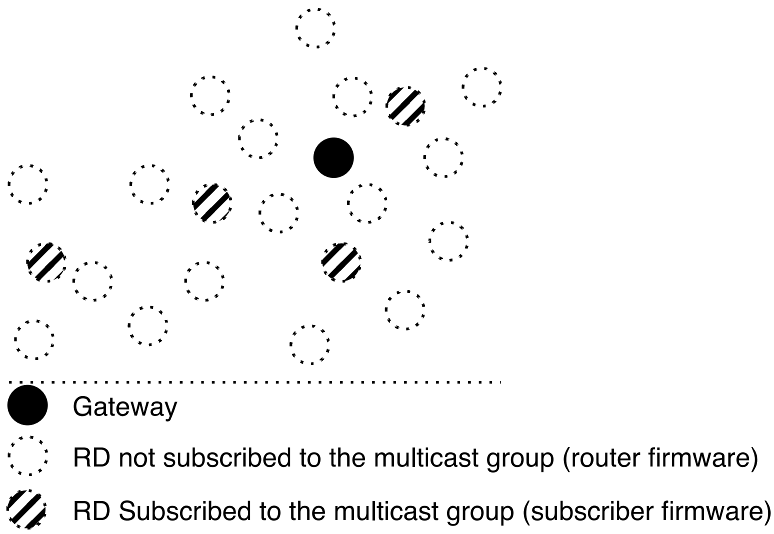

Figure 14 Indicative experiment topology

At the end of each run, the gateway application will request the number of multicast datagrams received by each of the RDs subscribed to the multicast group and will subsequently calculate Packet Delivery Ratio averages for different hop counts.

Network delay measurements are more complicated: Since RDs and the gateway will not have synchronised clocks, network delay can only be evaluated by measuring Round-Trip-Time (RTT). To measure network delay, we shall setup a deployment of a single multicast traffic subscriber and we will position it far from the traffic source, in order to achieve multi-hop communication. The RD will be programmed to reply to the sender of multicast datagrams using unicast. We will then send a single datagram from the gateway, await the reply from an RD and measure RTT before transmitting the next datagram. This will be done in order to avoid situations whereby the measurement method has an impact on the metric being evaluated (unicast replies causing delays to multicast delivery). The replies will be unicast, therefore even though RTT provides an indication of network delay per hop, it is incorrect to assume that each direction occupied 50% of the RTT. In the general case, downstram traffic (multicast from the gateway to the RD) will take longer to reach its destination than unicast upstream replies (from the RD to the gateway).

The entire set of permutations will be tested for both algorithms mentioned above.

3.13.4 RERUM architecture functional components involved/tested

On the Gateway:

- Communications and Network Manager: Routing

On RDs:

- Communication Management
  - Routing
  - IF selection

3.13.5 Foreseen experiment risks

Due to restrictions discussed in D2.1, evaluation will require that the software process generating multicast traffic be executed on the RERUM gateway (see D2.1, Sec 4.2, Contribution 22).

3.13.6 Timeplan

Indicative timeplan for this experiment:

- Implementation of IPv6 multicast forwarding and group management in the Contiki OS: done
- Implementation of experiments, including implementation of the gateway application: Until June 2015
- First set of lab tests: until August 2015.
- Evaluation of the results: September 2015

3.14 Lightweight Datagram Transport Layer Security (DTLS) Protocol

3.14.1 Purpose of the experiment

The goal of this experiment is to check behaviour of DTLS protocol in the environment, which is closer to real deployment scenarios. The experiments should investigate two major issues: performance of implemented (in lightweight fashion) cryptographic schemes and performance of DTLS protocol itself. There are many undefined factors of a lightweight DTLS implementation especially considering real deployment behaviour. It is important to select cryptographic schemes that will yield in the best performance at chosen security level. As the best performance (i.e. trade-off between factors) one can think of algorithm speed, code footprint or power consumption and all these metrics will be investigated in the experiment. Although cryptographic schemes plays almost the most important role in said protocol, their impact on overall protocol performance will be also under investigation, i.e., latency of overall handshake protocol in end-to-end setup, as well as packet retransmission impact on said latency in real wireless communication channel.

The DTLS protocol details and a set of possible cryptographic primitive choices are described in D3.1. Implementation will be carried on the real hardware platforms, i.e., RERUM-designed Re-Mote and more computationally powerful Gateway platform such as well-known Rasberry Pi or BeagleBone Black.

The experiment requires at least four Re-Mote nodes and one Gateway. All devices have to provide specified in D3.1 and in supported documents DTLS version 1.2 functionality. Since Bootstrapping mechanism will not be available in experiments we assume that all necessary key material is loaded into devices in advance.

3.14.2 KPIs

The KPIs that will be measured within this experiment are the following:

- Code footprint of cryptographic primitives,
- Performance of cryptographic primitives running on both Re-Mote platform and Gateway,
- Power consumption of cryptographic primitives, as well as overall power consumption of DTLS protocol,
- Overall latency of DTLS handshake in different scenarios, i.e., using symmetric and asymmetric schemes in end-to-end scenario.

3.14.3 Experimental scenarios

The experimental topology is depicted on Figure 15. It consists of one Gateway (Rasberry Pi or BeagleBone Black) and at least 4 Re-Mote nodes, configured in such a way that addresses the experiential scenarios. In particular:

- RD1 should be able to establish a direct communication link with RD4,
- RD1 should be able to establish indirect communication links with RD3 and with the Gateway,
- RD2 should be able to establish direct communication links with RD1, RD3 and the Gateway,
- RD3 should be able to establish direct communication links with RD2 the Gateway.

All communication links are based on IEEE 802.15.4.

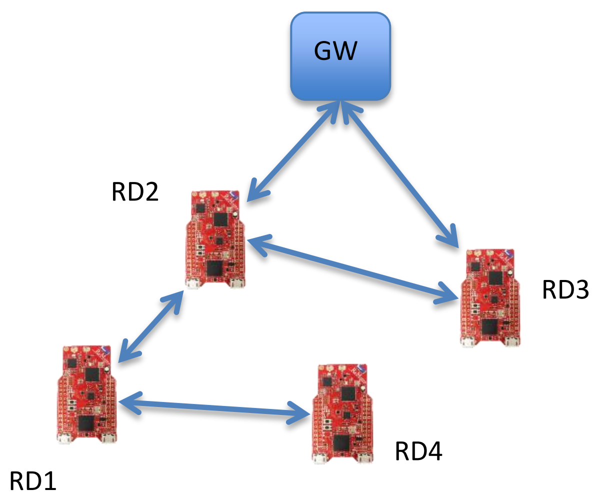

Figure 15 Network topology for testing DTLS

3.14.3.1 RD1-to-RD4 (single hop)

In this setup RD1 acts as a client and wants to communicate with the RD4, which acts as a server. DTLS performs mutual authentication with use of both symmetric and asymmetric schemes. There is a direct connection between RD1 and RD4, i.e., packets are not routed through any other device.

3.14.3.2 RD1-to-RD3 (end-to-end)

In this setup RD1 acts as a client and wants to communicate with the RD3, which acts as a server. DTLS performs mutual authentication with use of both symmetric and asymmetric schemes. There is no direct connection between RD1 and RD3, i.e., packets are routed through the other device (RD2).

3.14.3.3 RD3-to-GW (single hop)

In this setup RD1 acts as a client and wants to communicate with the GW, which acts as a server. DTLS performs mutual authentication with use of both symmetric and asymmetric schemes. There is a direct connection between RD1 and GW, i.e., packets are not routed through the other device.

3.14.3.4 RD1-to-GW (end-to-end)

In this setup RD1 acts as a client and wants to communicate with the GW, which acts as a server. DTLS performs mutual authentication with use of both symmetric and asymmetric schemes. There is no direct connection between RD1 and GW, i.e., packets are routed through the other device (RD2).

3.14.4 RERUM architecture functional components involved/tested

On RDs and the Gateway:

- DTLS modules (client and server)

Network monitor

3.14.5 Foreseen experiment risks

The significant risk comes from uncertainty of efficient cryptographic primitives implementations on said test platform. In the worst-case scenario, we could observe practically unacceptable results.

3.14.6 Timeplan

Indicative timeplan for this experiment:

- Implementation of DTLSv1.2 in the Contiki OS: done
- Implementation of experiments, including implementation of different cryptographic primitives: Until June 2015
- First set of lab trials: until August 2015.
- Evaluation of the results: September 2015

4 Proof-of-concept Field Trials

One of the most important activities of the project is the execution of trials in two large-scale real-world environments in the two participating Cities, i.e., Tarragona and Heraklion. The trials will be split into two phases. During each of the two phases, the cities will execute different use-cases (both indoors and outdoors). During phase 1 Heraklion will execute UC-O1 and UC-I1 while Tarragona will execute UC-O2 and UC-I2 and the reverse in phase 2.

4.1 Heraklion Trials

4.1.1 Phase-1 Trials

4.1.1.1 UC-O1: Outdoor - Smart Transportation

4.1.1.1.1 Definition

The goal of UC-O1 trials will be to collect data from moving vehicles around the city and exploit them in order to help the citizens and the city to improve their planning and transportation activities. More specifically, the trials will focus primarily on data collection from public transportation vehicles (e.g., buses) or volunteers (in the second phase) and will collect the following data:

- Vehicle Type
- Location
- Speed, Accuracy, and Heading
- Travel Time

The use-case is focused on methods for collecting traffic data, over heterogeneous networks of various sensors and RERUM Devices, which can then be utilized to perform real time traffic estimation for intelligent transportation systems in Smart Cities. The main objectives of this trial are the following:

- Perform measurements throughout the cities
- Visualize traffic measurements
- Ensure the trustworthy exchange of information between the RERUM Devices and the application
- Preserve the privacy of user data and ensure the trustworthy and secure transmission of user data to the applications. Always anonymise user data before transmission (at smart object level)

4.1.1.1.2 Mapping of UC ecosystem components to trial functionality and technical components

Table 2 Heraklion UC-O1 main components, describes the main components deployed for the UC-O1.

Table 2 Heraklion UC-O1 main components

Component	Description	Physical installation
Vehicles	Public transportation vehicles. Specific routes will be selected.	N/A
Sensors	Sensing elements of the type described in Table 3.	
RERUM Devices	Smartphones will be utilized as RDs. The requirements that have to be satisfied are the sensing elements of Table 3 and the	Installed in buses

Component	Description	Physical installation
	network connectivity which shall include 3G connectivity.	
Network gateway and intermediate data aggregation points (i.e. cluster heads)	RDs could be used as Gateways. However, during 1st phase trials gateways will not be used. GWs functionality will be examined during phase 2.	Potentially installed on buses
Middleware server	The MW server shall be responsible for the communication of the RDs with the application servers. It will be installed in Heraklion premises.	Heraklion premises
Application server	The application server shall be responsible for the transport services (e.g., traffic estimation, visualization of real-time traffic state). Visualization outcomes of traffic estimation shall be available on a web page. Available for all citizens	Heraklion premises

Table 3 Sensor types for Heraklion UC-O1, describes the sensors used in the UC-O1.

Table 3 Sensor types for Heraklion UC-O1

Sensor	Description
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.
GPS_RECEIVER	Measures the location in the WGS84 reference system as well as point speed, orientation and time.
WIFI_MODULE	Captures the MAC address and RSS of current and nearby WiFi access points.
CELLULAR_MODULE	Measures the Cell Id and RSS of current and nearby cellular base stations.

4.1.1.1.3 Deployment of components

Figure 16 below shows the overview of the architectural deployment for UC-O1.

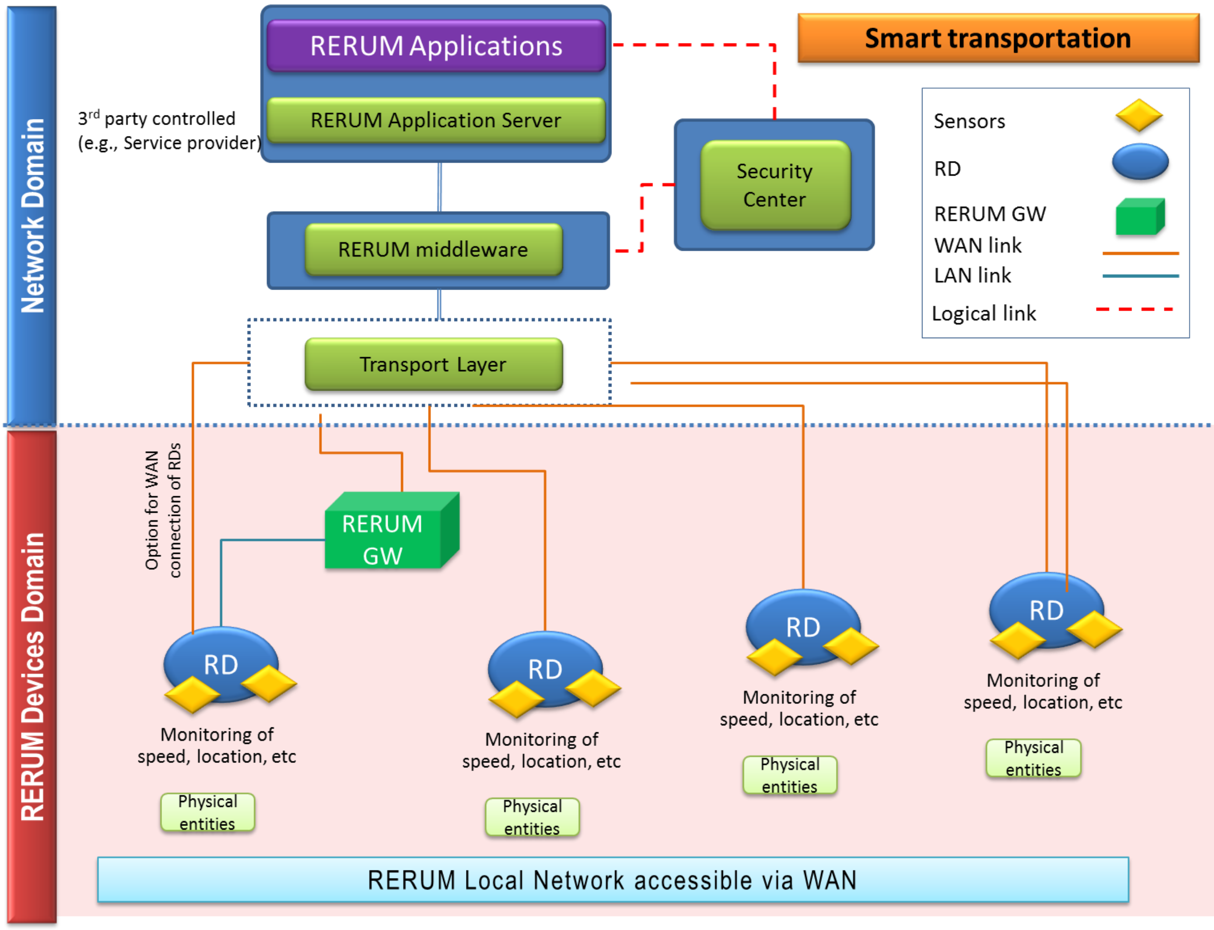

Figure 16 Heraklion UC-O1 Smart transportation high-level overview

Table 4 illustrates the interfaces between the components for UC-O1

Table 4 Interfaces between Trial components (Heraklion)

Components	Smartphone	Gateway (optional)	Middleware	Application Server
Smartphone	n/a	**Connectivity**: 802.11b/g **Scope**: Traffic aggregation, Packet forwarding, Energy savings for smartphones	**Connectivity**: Transport technology: 3G/4G Application layer protocol: REST based on http.	**Connectivity**: Transport technology: 3G/4G Application layer protocol: REST based on http.
Gateway (optional)	**Connectivity**: 802.11b/g **Scope**: Traffic aggregation, Packet forwarding, Energy savings for smartphones	n/a	**Connectivity**: Technology: 3G/4G Application layer protocol: REST based on http	**Connectivity**: Transport technology: 3G/4G Application layer protocol: REST based on http.
Application	**Connectivity**: Transport	**Connectivity**: Transport technology:	**Connectivity**: Transport	n/a

Components	Smartphone	Gateway (optional)	Middleware	Application Server
server	technology: 3G/4G Application layer protocol: REST based on http.	3G/4G Application layer protocol: REST based on http.	technology: 3G/4G Application layer protocol: REST based on http.	

Bus routes:

The public transportation company in Heraklion serves 31 routes. The trial will focus on specific routes, taking into account the limitation on the number of smart-devices that are available for the trials. After discussions with the city of Heraklion, we have identified that the initial interest of the trials will be on the bus lines 2, 6, 8, 10, 11, 12, 21 and 31, because they pass quite frequently from the basic arteries of interest.

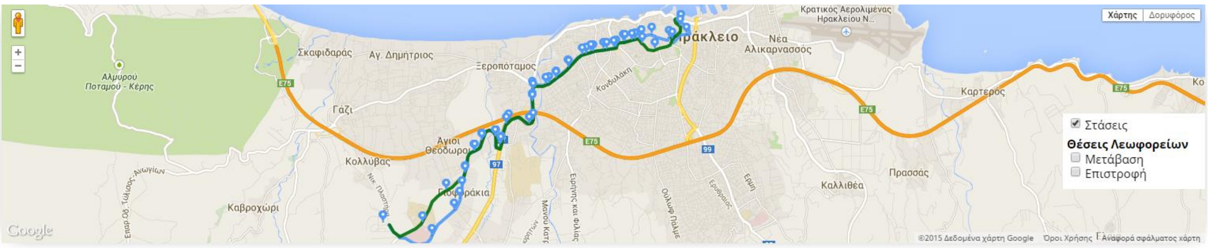

Figure 17 Bus route from Port to FORTH (line 8)

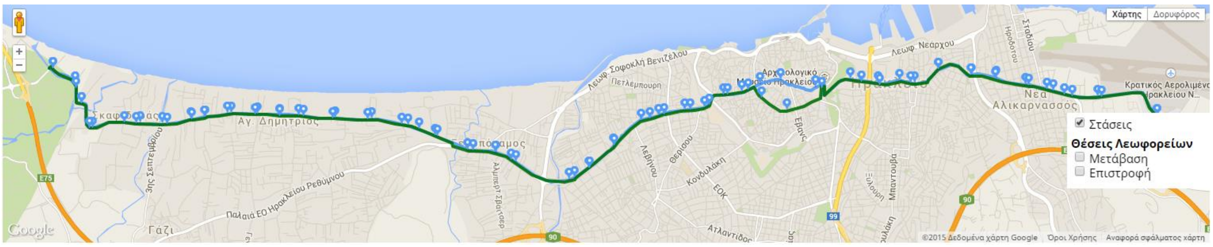

Figure 18 Bus route from Airport to Ammoudara beach (line 6)

Table 5 Heraklion bus routes that will be used (UC-O1), includes the devices installed on the selected bus routes.

Table 5 Heraklion bus routes that will be used (UC-O1)

Route	Description
2	One smartphone running the Traffic Estimation Application per bus that takes this route (the buses are not dedicated only to a specific route, they change even randomly according to the need of the schedule)
6	-//-
8	-//-
10	-//-
11	-//-
12	-//-
21	-//-

Route	Description
31	-//-

4.1.1.1.4 Scenarios description

The tables below include the scenarios that will be implemented in the UC-O1 trials in Heraklion

Table 6 Scenario UC-O1$_A$

Purpose of the scenario	The purpose of the scenario is to evaluate the RERUM energy efficiency mechanisms for traffic estimation applications.
Eval. criterion ID	ST.EF.1
KPIs	Loss of battery % per operational hour, per operation session
Scenario Description	The end-users will be requested to answer specific questionnaires related to the energy efficiency of the Traffic Estimation application and how it affects the battery lifetime of smartphones.
Topology	Same as the generic UC-O1 topology (Figure 16)

Table 7 Scenario UC-O1$_B$

Purpose of the scenario	The purpose of the scenario is to evaluate the RERUM processing efficiency mechanisms for traffic estimation applications.
Eval. criterion ID	ST.EF.2
KPIs	Keep the CPU % of the app as low as possible while collecting and transmitting
Scenario Description	The end-users will answer question on observing significant glitches in the Quality of Experience when the app is not in the foreground after installing the Traffic estimation app
Topology	Same as the generic UC-O1 topology (Figure 16)

Table 8 Scenario UC-O1$_C$

Purpose of the scenario	The purpose of the scenario is to evaluate the uptime of the Smart Transportation application once the RERUM middleware is used with them.
Eval. criterion ID	ST.PE.1
KPIs	The target is to investigate whether the app uptime that is independent of network and load
Scenario Description	The end-users will answer questions regarding how often they got error messages that required them to re-start the application.
Topology	Same as the generic UC-O1 topology (Figure 16)

4.1.1.1.5 Requirements and dependencies

The RD in this UC trial are android based smartphones that run RERUM application. Due to the vast amount of combinations of hardware and software versions available on the market for Android smartphones, using arbitrary devices it can be a difficult task within the project to assure good quality of tests in the trials. To address this issue we will provide a list of validated smartphones and their expected performance in the trials. The current list can be seen in Table 9 and it will be continuously updated. LiU will, furthermore, provide timely validation of any device proposed by the city.

In the trials the demo application is intended to demonstrate the RERUM platform/architecture in a traffic management use case. The use case is limited to traffic estimation proof-of-concept, over the RERUM-collected data.

Collection of data is carried out with the help of vehicle-mounted devices and devices carried by citizens. There are 2 categories of users:

- Public transportation dedicated to specific routes (as per 4.1.1.1.3)
  - The quality of traffic estimation is directly affected by the amount of data collected.
  - Consider deploying smart-phones on a minimum 12 routes.
- Participatory group of users that use smartphones
  - Users are requested to use smart-phones from the set of devices validated by LiU, Table 9, prior to trial and deployment.
  - The users are instructed to use only when driving their car with the help of Start-Stop button in the application.

Table 9 Validation of smart-phones

Device	Manufacturer	Android Version	Test result
Nexus -5	LG	5.0.1	OK
Nexus-4	LG	5.0.1	OK
Moto-E	Motorola	4.4.2	OK
Moto-G	Motorola	4.4.2	OK
Samsung Galaxy Young 2	Samsung	4.4.2	OK
Samsung Galaxy S5	Samsung	4.4.2	OK
Samsung Galaxy S3	Samsung	4.3	Issues exist regarding some features.
Sony Xperia Z2	Sony	4.4.2	OK
Samsung Xcover 2	Samsung	4.1.1	Currently not fully supported
Samsung Galaxy Y	Samsung	2.3	Currently not fully supported
HTC One	HTC	4.1.1	OK

4.1.1.1.6 Scheduling of the activities

Table 10 Heraklion's scheduling activities for UC-O1

Date	Actions

Date	Actions
End of May 2015	A first version of the mobile app from LiU (without SAGs algorithm) will be ready.
End of May 2015	The server side application will be ready
End of July 2015	There will be an internal test (in our – FORTH's/Cyta's devices) until end of July to test the application and fix things
September 2015 and onwards	When everything is ready, we'll install the devices on the buses/taxis in July (to use this for summer promotion

4.1.1.1.7 Risks and related solutions

- Deployment delays:
- Low participation: Quality is directly proportional to data collected. Increase the participation of users to collect more data.
- Physical safety of the device: protection using hard case to prevent damage due to accidental impacts of falling on hard surfaces.
- Safety of devices on public transport: Ensure proper safety to prevent theft or accidental misplacement of the device.
- Power connectivity: Ensure the device is connected to power supply on the busses.
- Proper operation of the application: Proper training for the user to understand when the application starts and stops.
- Collection of unnecessary data: Stop application when the user is out of the vehicle.

4.1.1.2 UC-I1: Indoor - Home energy management

4.1.1.2.1 Definition

The goal of UC-I1 trials will be to monitor the energy consumption of high-consuming devices within government buildings in the municipality of Heraklion. More specifically, the trials will focus on two specific buildings, i.e., **Vikelaia Library** (a very new building) and **Androgeo building** (a very old building). The goal would be also to make a comparison for the energy consumption of the two buildings. The monitoring will focus on the following:

- Energy consumption of Air Conditioners (A/C)s
- Energy consumption of Personal Computers (PC)s
- Energy consumption of lighting

Furthermore, it will be investigated whether federations can be demonstrated, such as the cooperation between energy monitoring devices and actuators (for example monitor the status of windows and make recommendations for actions, e.g., turn-off ACs when windows are open).
The collected data will be forwarded to an application server, where they will be processed in order to be usable by an end-user (e.g., building administrator) in terms of:

- Real-time energy monitoring of requested device(s)
- Extraction of statistical results for the energy consumption of the devices

4.1.1.2.2 Mapping of UC ecosystem components to trial functionality and technical components

The components that will be used in UC-I1 trials as well as their roles are given in Table 11.

Table 11 Heraklion's UC-I1 main components

Component	Description
Sensors	The sensors will measure: • the operating electrical current/voltage of devices • the ambient light in a room • motion of objects (e.g., windows and doors).
RERUM Devices	They have the capability to send the sensed information (via wires or wirelessly) to other network nodes (e.g., RDs or gateways) for further processing. In UC-I1, RDs include smart home electrical appliances, RERUM Devices 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 will serve 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).
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).

4.1.1.2.3 Deployment of components

The RDs will be equipped with the corresponding sensors in order to monitor

- The energy consumption of **individual** devices and appliances (personal computers, air conditioners and heating electrical units)
- The energy consumption **of groups of devices**/appliances through the monitoring of the consumption of entire electrical panels, e.g., the electrical panel that controls the power supply of a building's floor.
- the ambient **light** in rooms
- **motion** of objects (e.g., windows and doors).

The RDs will transmit the sensed data to a RERUM GW, which will be deployed within the buildings. The number of RERUM GWs will depend on the indoor propagation conditions which affect the quality of the connection (e.g., bit rate, connection reliability). The transmission protocol will be 802.11a/b/g/n. The RERUM GW will aggregate the transmitted data and forward them to the application server, after the secure connection with the RERUM MW and the application server has been successfully established.

The RERUM Gateway will be connected via Ethernet or 802.11a/b/g/n to an Internet access point, which will use xDSL or/and cellular (GPRS) as the transmission protocols.

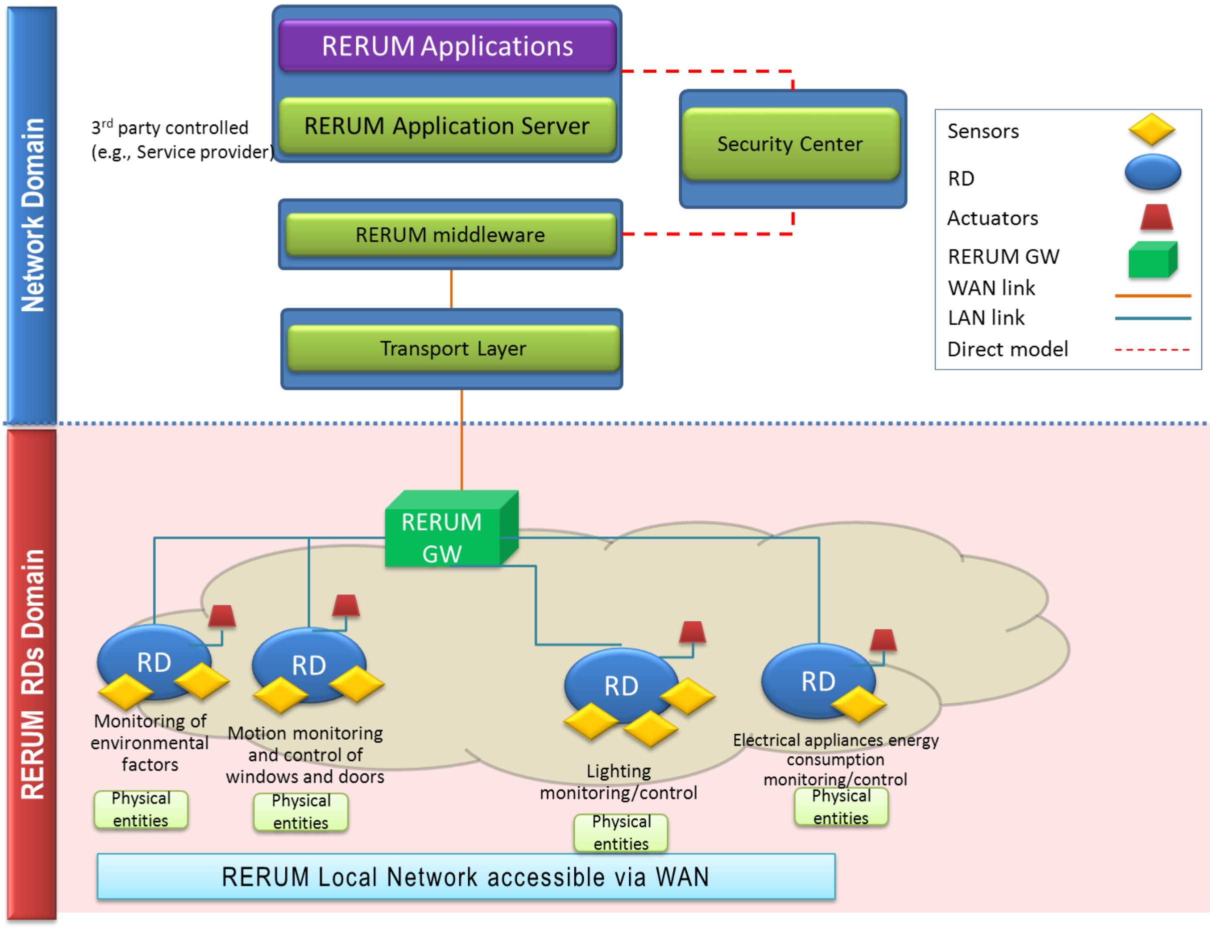

Figure 19 Home energy management high-level overview (Heraklion)

The application server will be an Apache Web server with PHP and Round-robin Database (RRD) implemented on it. RDs are particularly designed for handling time-series data like network bandwidth, temperatures, etc. The acquired data are stored in a circular buffer based database. The RRDtool which will be installed in the server assumes time-variable data in intervals of a certain length. This interval is specified upon creation of an RRD file and cannot be changed afterwards. Given the fact that the sensed data will be energy consumption data, this interval will be in the order of minutes (e.g., 5-10 minutes).

The application server will read the data from the RDs and store them on the RRD. Besides the RRDtool, Cacti will also run on the application server, which will be used as a graphing tool. Cacti will allow a user to poll the monitored data at predetermined intervals and graph the resulting data. It will be used both for graphing real time-series data and data statistics.

In Figure 20 and Figure 21 two examples of what will be displayed in the web interface of the application server are given. The RRDtool and the Cacti give the ability for the user to view the network deployment (e.g., RERUM GWs, devices, etc.) and the real-time data monitoring.

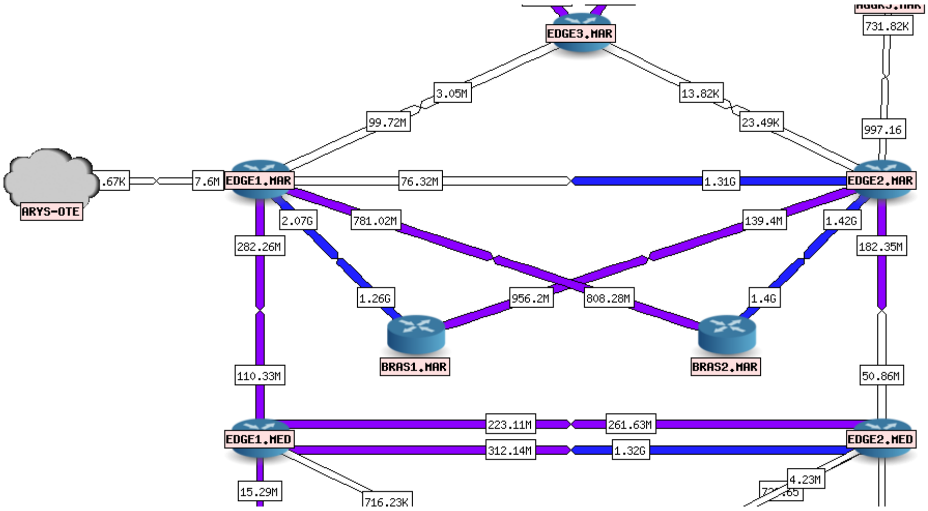

Figure 20 Cacti network deployment view (example)

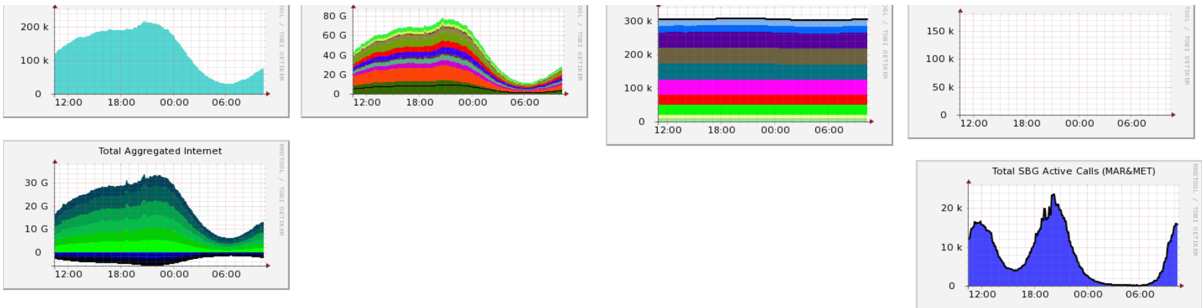

Figure 21 Real-time monitoring using RRDtool and Cacti (example)

Table 12 Interfaces between Trial components (Heraklion)

Components	RERUM Device	Gateway	Middleware	Application Server
RERUM device	n/a	**Connectivity**: IEEE 802.15.4 **Scope**: Traffic aggregation, Packet forwarding, Energy savings for devices	n/a	n/a
Gateway	**Connectivity**: IEEE 802.11a/b/g/n IEEE 802.15.4 **Scope**: Traffic aggregation, Packet forwarding, Energy savings for devices	n/a	**Connectivity**: Transport technology: xDSL Application layer protocol: REST based on http.	n/a

Components	RERUM Device	Gateway	Middleware	Application Server
Middleware	n/a	**Connectivity**: Transport technology: xDSL Application layer protocol: REST based on http	**n/a**	**Connectivity**: Transport technology: irrelevant Application layer protocol: REST based on http
Application Server	n/a	n/a	**Connectivity**: Transport technology: xDSL Application layer protocol: REST based on http	**n/a**

Table 13 Summary of the devices measurements for UC-I1 (Energy monitoring), shows the sensors and devices deployed at each location:

Table 13 Summary of the devices measurements for UC-I1 (Energy monitoring)

Location	Measurements			Number of components	
	Energy consumption	**Presence**	**Light Sensor**	**RD**	**GW**
Vikelaia Library	Yes	Yes	Yes	20	2
Androgeo building	Yes	Yes	Yes	20	2

Figure 22 The Vikelaia Library

Figure 23 The building at Androgeo street

4.1.1.2.4 Scenarios description

The tables below include the scenarios that will be implemented in the UC-I1 trials in Heraklion

Table 14 Scenario UC-I1$_A$

Purpose of the scenario	The purpose of the scenario is to evaluate the RERUM authorization process based on user roles
Eval. criterion ID	AL.AU.2
KPIs	Success of policy control
Scenario Description	Define a user attribute role in the Identity platform or make sure that you use an already existing one in the following step For each zone of the building subject to be accessed by a different user, upload in the system 1 security policy that checks the proper role for that zone Check the policy with different users that have different values for that attribute by inspecting the logs of the authorization engine
Topology	Figure 24, Figure 25

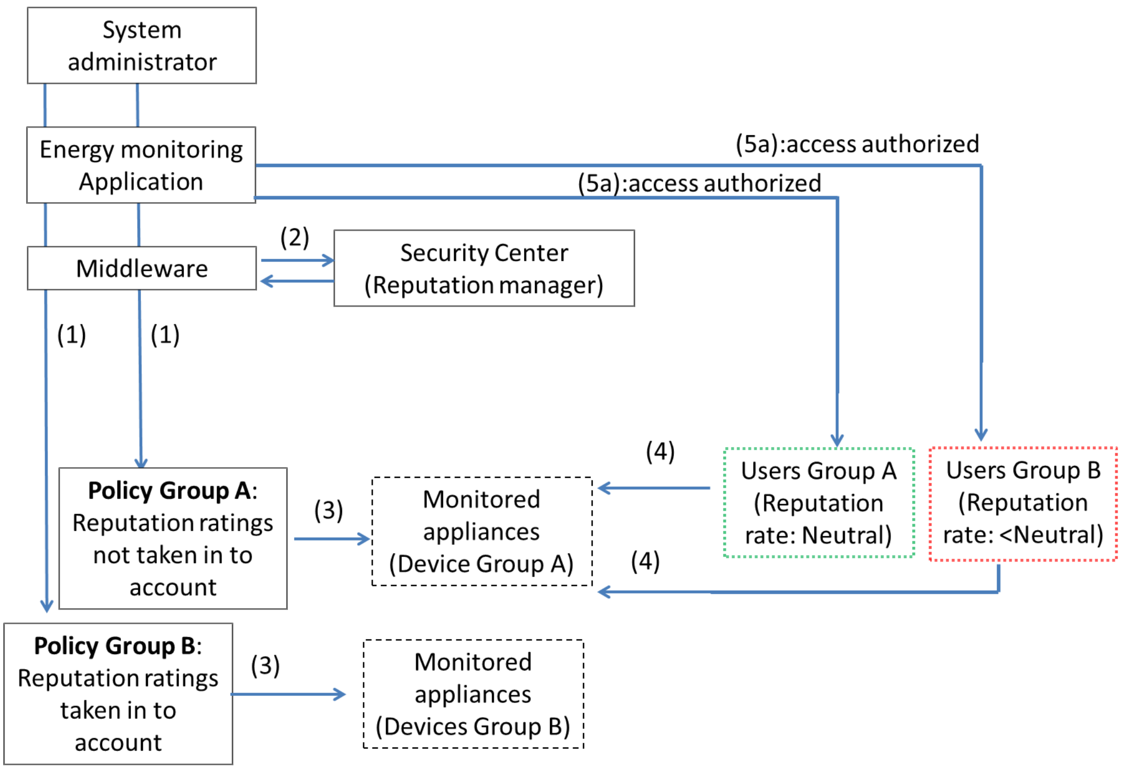

Figure 24 Scenario UC-I2$_A$ (No group policy applied)

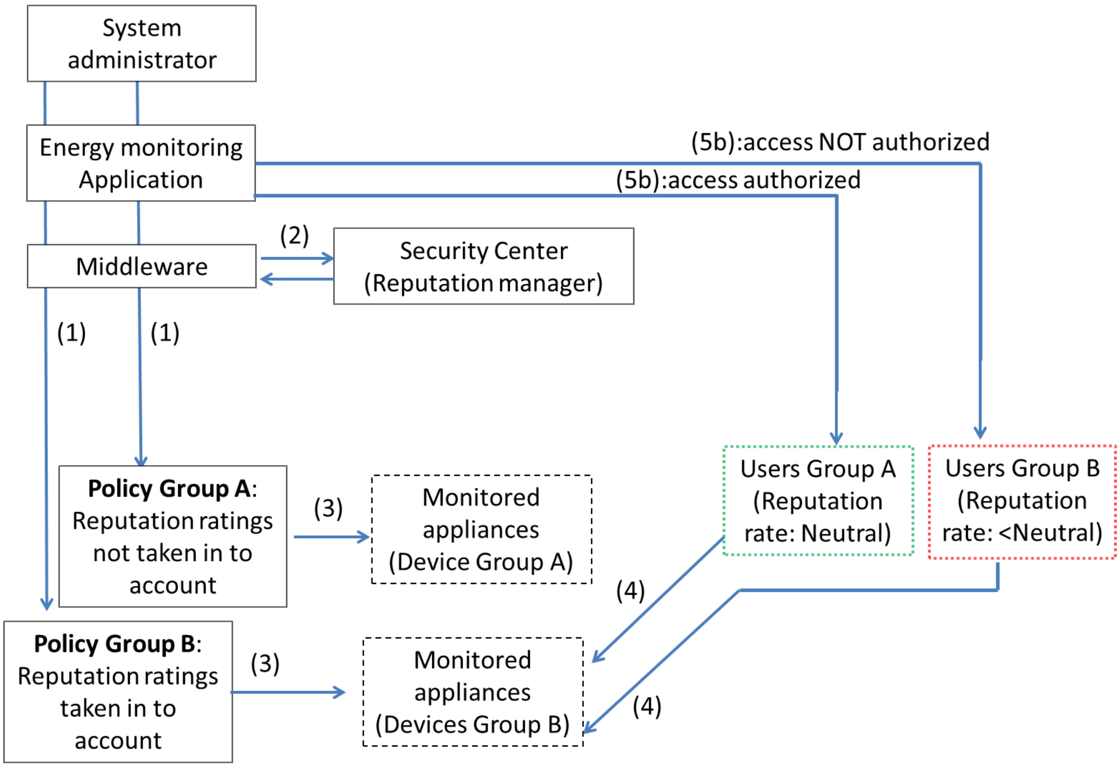

Figure 25 Scenario UC-I2$_A$ (Group policy applied)

This scenario will try to check the access of distinct users with different roles to the distinct zones of the public buildings. For each zone supposed to be accessed by different people it will be necessary to create proper policy files that allow accessing them only to those users that have the proper role associated.

4.1.1.2.5 Requirements and dependencies

N/A for this UC.

4.1.1.2.6 Scheduling of the activities

Table 15 Heraklion's scheduling activities for UC-I2

Date	Actions
End of May 2015	The application server will be ready. The connection between the necessary RERUM architectural components and the respective protocols' functionalities will be tested.
September 2015 - February 2016	Trials begin to run live. The support will be continuous in order to • gather the necessary information for the evaluation of the trial • face any problems that may occur • improve any functionalities and mechanisms
March 2016	End of 1st phase trials. A report will be created with the results of the trials, the difficulties that have been

Date	Actions
	encountered, suggested improvements, etc. This report will feed Tarragona's UC-I1 trials.

4.1.1.2.7 Risks and related solutions

The possible risks for this use case are given in Table 16.

Table 16 Possible risks for UC-I1 (Heraklion)

Possible Risk	Probability to occur	Suggested solution
Granularity level for RDs installation (e.g., installation on personal appliances) not accepted by building administration	Low, since an oral agreement is already in place.	Granularity level for RDs installation will gradually change, e.g., from individual devices to rooms, or floors, etc. in order to reach an agreement with the building administration.
Granularity level for RDs installation (e.g., installation on personal appliances) not accepted by building employees,	Low, since an oral agreement is already in place.	Educational seminars will take place in order to inform the employees about how RERUM preserves their privacy. In case the employees still do not accept the granularity level, then it will change e.g., from individual devices to rooms, or floors, etc. in order to reach an agreement with the employees.

4.1.2 Phase-2 Trials

4.1.2.1 UC-O2: Outdoor - Environmental monitoring

4.1.2.1.1 Definition

The goal of UC-02 trials will be 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. The trials will focus on the measurements of:

- The air (CO, CO2, NO2, Temperature, RH)
- PM10, PM2.5
- The noise
- The EMF radiation

The collected data will be forwarded to an application server, where they will be processed in order to be usable by an end-user (e.g., building administrator) in terms of:

- Real-time monitoring of requested environmental factors
- Extraction of statistical results for the energy consumption of the devices

4.1.2.1.2 Mapping of UC ecosystem components to trial functionality and technical components

Table 17 UC-I1 main components (Heraklion)

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 18 for further details on sensors used in UC-O2.
RERUM Devices	The RDs 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 RDs 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. RDs communicate wirelessly, using 6LoWPAN over IEEE 802.15.4 (on the specified frequency bands). RDs are composed of: • A RF IEEE 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 RD 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. • Noise and rain: according also to the EC directives [5], 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	Due to the limited communication range and bandwidth restrictions of the RDs' wireless communication technology, it is necessary to add gateways or cluster heads close to RDs to communicate/fuse the gathered data to the application server over the internet. Thus, a gateway will be equipped with an IEEE 802.15.4 interface for communication with the

Component	Description
nodes)	RDs 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.

Table 18 Sensor types for UC-O2 (Heraklion)

Sensor	Sensing elements	Description	Common Uses
Air Quality	SO_2 NO_X O_3 VOC PM_{10}	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	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	Measures the electromagnetic radiation	Detect abnormal EM radiation

4.1.2.1.3 Deployment of components

The RDs that will be installed in the city locations will transmit the sensed data to a RERUM GW, which will be installed in the proximity of the RDs. The number of RERUM GWs will depend on the propagation conditions which affect the quality of the connection (e.g., bit rate, connection reliability). The transmission protocol will be 802.11a/b/g/n. The RERUM GW will aggregate the transmitted data and forward them to the application server, after the secure connection with the RERUM MW and the application server has been successfully established.

The RERUM Gateway will be connected via Ethernet or 802.11a/b/g/n to an Internet access point, which will use cellular (GPRS) as the transmission protocols.

The application server will be an Apache Web server with PHP and Round-robin Database (RRD) implemented on it. RDs are particularly designed for handling time-series data like network bandwidth, temperatures, etc. The acquired data are stored in a circular buffer based database. The RRDtool which will be installed in the server assumes time-variable data in intervals of a certain length. This interval is specified upon creation of an RRD file and cannot be changed afterwards. Given the fact that the sensed data will be related to environmental factors that may be critical for citizens' health the measuring period may be of the order for seconds.

The application server will read the data from the RDs and store them on the RRD. Besides the RRDtool, Cacti will also run on the application server, which will be used as a graphing tool. Cacti will allow a user to poll the monitored data at predetermined intervals and graph the resulting data. It will be used both for graphing real time-series data and data statistics.

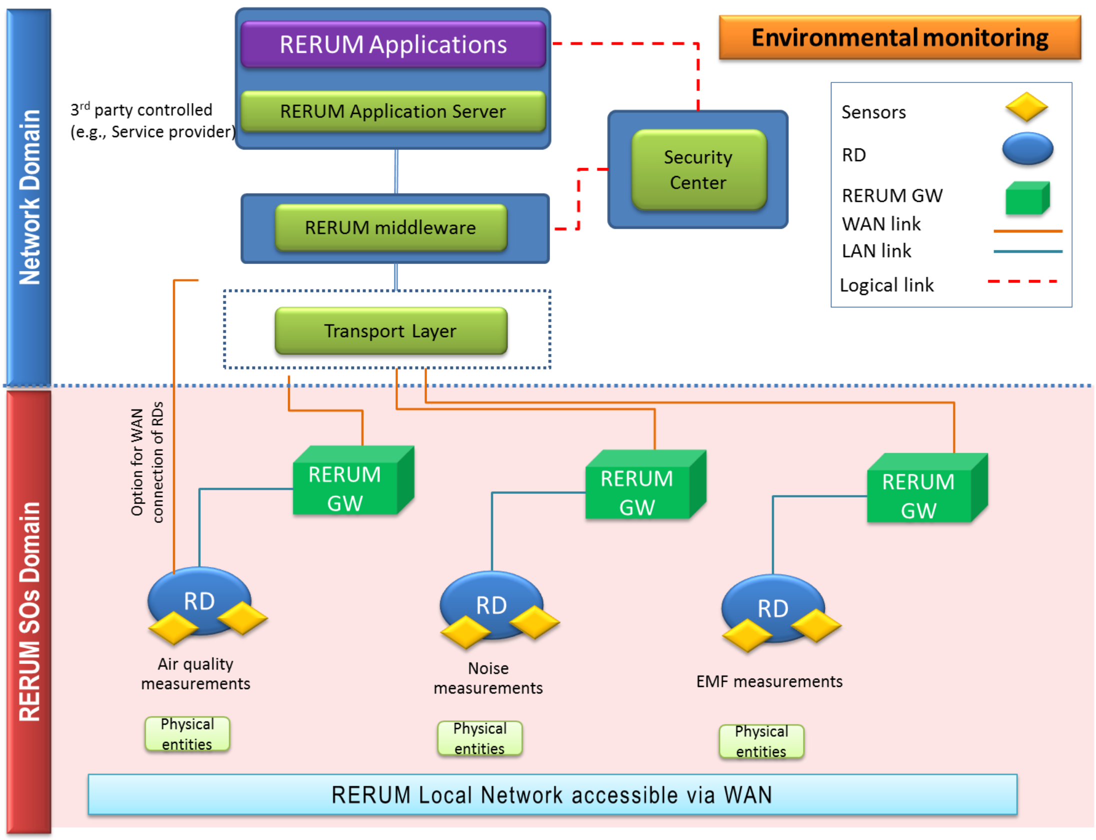

Figure 26 Environmental monitoring high-level overview (Heraklion)

Table 19 Interfaces between Trial components (Heraklion)

Components	RERUM Device	Gateway	Middleware	Application Server
RERUM device	n/a	**Connectivity**: IEEE 802.11a/b/g/n IEEE 802.15.4 **Scope**: Traffic aggregation, Packet forwarding, Energy savings for devices	n/a	n/a
Gateway	**Connectivity**: IEEE 802.11a/b/g/n IEEE 802.15.4 **Scope**: Traffic aggregation,	n/a	**Connectivity**: Technology: GPRS ApplicationREST based on HTTP.	n/a

Components	RERUM Device	Gateway	Middleware	Application Server
	Packet forwarding, Energy savings for devices			
Middleware	n/a	**Connectivity**: Technology: GPRS ApplicationREST based on HTTP.	**n/a**	**Connectivity**: Technology: irrelevant ApplicationREST based on http.
Application Server	n/a	n/a	**Connectivity**: Technology: GPRS ApplicationREST based on HTTP.	**n/a**

The devices will be installed either on buses or at fixed places:

- On buses (if possible). The application on the devices will be programed to take measurements only when the bus stops at the bus-stops (to ensure that the data will not be affected by the movement of the bus).
- Fixed places:
    - At the square outside the municipalities building (a very crowded area)
    - At the Eleftherias square.
    - Outside the Museum of Natural History (next to the sea).
    - At the Koules Fortress next to the sea.
    - At the Pancretan stadium.
    - At the Panagitsa square.
    - At the Kazantzakis park.

At each one of these places, at least 5 sensors will be installed at various points. The devices will be connected to the open WiFi of the municipality.

Table 20 Sensor types for UC-O2 (Environmental outdoor), shows the sensors and devices deployed at each location:

Table 20 Sensor types for UC-O2 (Environmental outdoor)

Location	Measurements – sensors			Number of devices	
	Air quality	Noise	Weather	RD	GW
At the square outside the municipalities building	Yes	Yes	No	4	1
Eleftherias square	Yes	Yes	No	4	1
Outside the Museum of Natural History	Yes	Yes	No	4	1

Location	Measurements – sensors			Number of devices	
	Air quality	Noise	Weather	RD	GW
Koules Fortress	Yes	Yes	No	4	1
Pancretan stadium	Yes	Yes	No	4	1
Panagitsa square	Yes	Yes	No	4	1
Kazantzakis park	Yes	Yes	No	4	1

Figure 27 Placement of sensors for UC-O2 trials (Heraklion)

4.1.2.1.4 Scenarios description

The tables below include the scenarios that will be implemented in the UC-O2 trials in Heraklion

Table 21 Scenario UC-O2$_A$

Purpose of the scenario	The purpose of the scenario is to demonstrate how M/W functions can leverage layer 3 multicast in order to improve network performance and decrease energy consumption, ultimately increasing deployment lifetime
Eval. criterion ID	AL.PE.5
KPIs	• Reliability by measuring packet loss / packet delivery ratio. • Network Delay (<1 sec per network hop) • Suitability for embedded devices by measuring code size and RAM requirements. Targets for the RE-Mote platform: <3 KB and <3 KB respectively)
Scenario Description	• A set of RDs will subscribe to a multicast group. • A RERUM gateway will be selected as the source of multicast traffic, with destination to this multicast group.
Topology	Figure 28

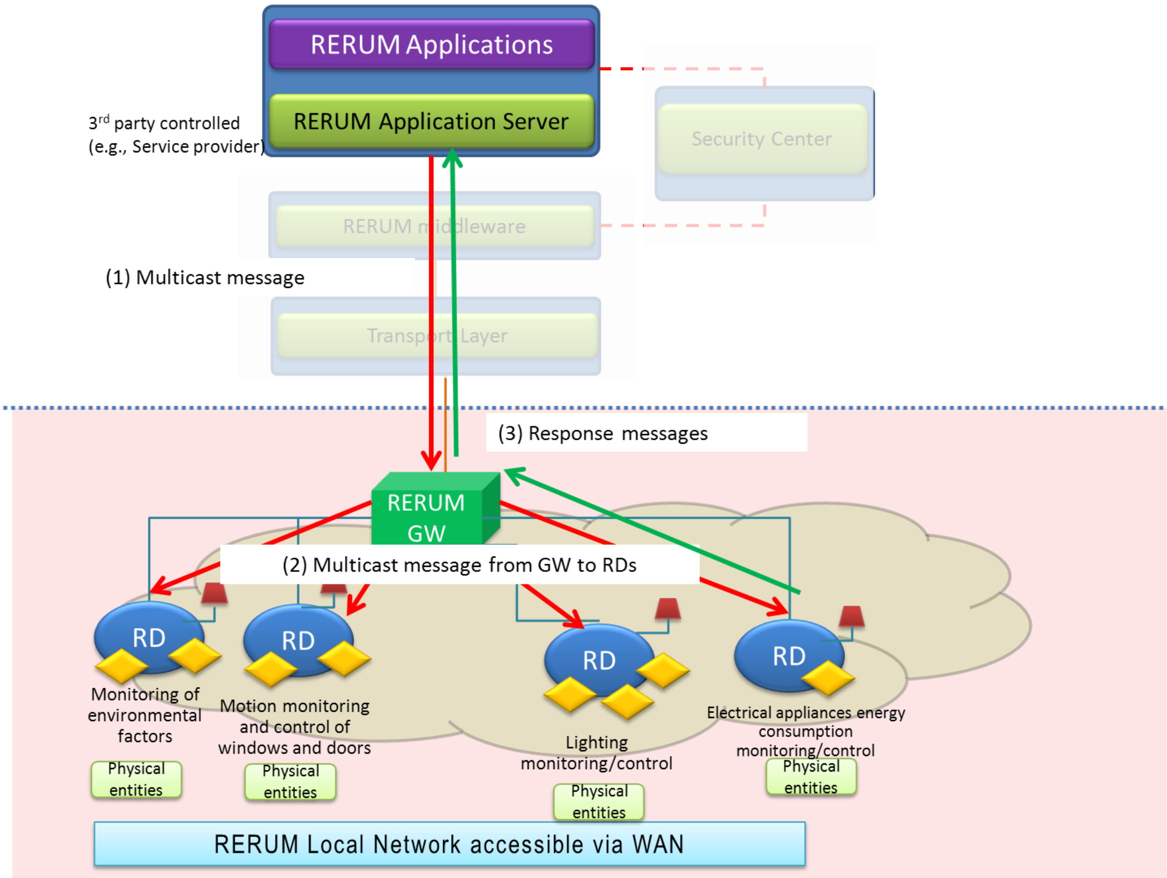

Figure 28 Scenario UC-O2$_A$ (6LoWPAN Multicast)

In this scenario the end-user will send a message to a group of RDs (for example request measurement values from all noise sensors in a specific area). Those RDs will have previously subscribed to a multicast group. The request will arrive at the serving GW, which then will send a multicast message to the RDs that should get the request. Then the following metrics will be measured:

- Network Delay which will be evaluated by measuring Round-Trip-Time (RTT)
- Reliability which will be evaluated by measuring Packet Delivery Ratio on each multicast group subscriber.

Table 22 Scenario UC-O2$_B$

Purpose of the scenario	The purpose of the scenario is to demonstrate how RE-Mote system update will happen through OAP and PRRS.
Eval. criterion ID	AL.SE.4
KPIs	Success of system update.
Scenario Description	• Search the firmware using the tags predefined in the form at the endpoint '/PRRS-webgui'. • Select the concrete firmware to use. • Select the concrete VRD or VRD Federation to update, previously defined in the GVO Manager. • Confirm the update. • Wait for the success response from the target device.
Topology	

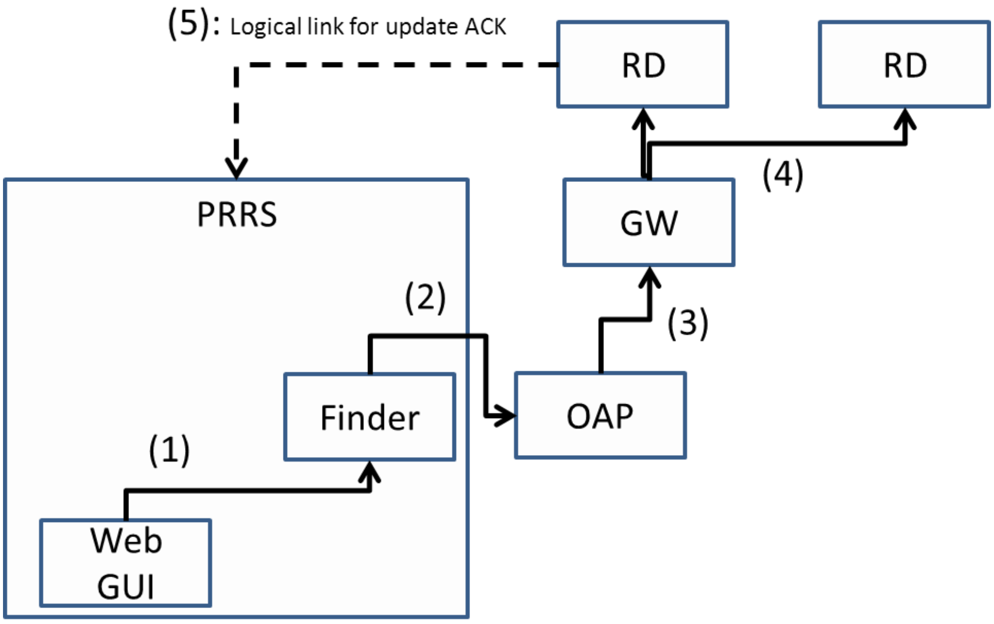

Figure 29 Scenario UC-O2$_A$ (OAP updates)

4.1.2.1.5 Requirements and dependencies

There is a requirement for guaranteed QoS, so we'll discuss with the technician responsible for maintaining the APs to see if hidden SSIDs can be used at the APs to connect the sensors. VPNs will be used with the extra SSIDs.

4.1.2.1.6 Scheduling of the activities

Table 23 Heraklion's scheduling activities for UC-O2

Date	Actions
End of January 2016	The application server will be ready. The connection between the necessary RERUM architectural components and the respective protocols' functionalities will be tested.
End of February 2016	The RDs will be deployed in the specified places and the connectivity with the application server and the RERUM architectural components will be tested.
March 2016	Trials begin to run live. The support will be continuous in order to • Assess the feedback that will be provided by Tarragona, regarding the UC-O2 trials in 1st phase. • gather the necessary information for the evaluation of the trial • face any problems that may occur • improve any functionalities and mechanisms
July 2016	End of 2nd phase trials. Final evaluation. Cross evaluation.

4.1.2.1.7 Risks and related solutions

The possible risks for this use case are given in Table 24.

Table 24 Possible risks for UC-O1 (Heraklion)

Possible Risk	Probability to occur	Suggested solution
Networking problems.	Low	Two radio access network interfaces will be used for increasing the network reliability.
RDs are destroyed because of vandalism.	Low	Wifi access points are already installed across the municipality and no actions of vandalism have been reported.

4.1.2.2 UC-I2: Indoor - Comfort quality monitoring

4.1.2.2.1 Definition

The goal of UC-I1 trials will be to provide measures for the quality of life in indoor environments (the home comfort). 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.

4.1.2.2.2 Mapping of UC ecosystem components to trial functionality and technical components

Table 25 UC-I1 main components (Heraklion)

Component	Description
Sensors	The sensors will measure: • Temperature, RH • CO2, CO • PM10, PM2.5 • EMF radiation
RERUM Devices	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. RDs communicate mostly wirelessly, using 6LoWPAN over IEEE 802.15.4 or wires through Ethernet connectivity. Most of the RDs 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 RDs are also used as supports for the devices. RERUM Devices are composed of: • An RF IEEE 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.
Gateway	It will serve 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.
Application server	It is responsible for the end-user services. Depending on the implementation options, it may be accessed through an external network (e.g., cellular network).

4.1.2.2.3 Deployment of components

The devices will be installed at the following places.

- The KEP at the ground floor of the municipality building (a place to serve the citizens applications/questions/etc.) always crowded and next to restaurants/café.
- The town hall.
- The archeological museum.
- One of the buildings of the city technical agency (also crowded most of the time)

At least 5 sensors will be installed at each place – there is a requirement to not take average measurements from these sensors, but to transmit the exact values to the server.

The RDs will transmit the sensed data to a RERUM GW, that will be installed in the proximity of the RDs. The number of RERUM GWs will depend on the propagation conditions which affect the quality of the connection (e.g., bit rate, connection reliability). The transmission protocol will be 802.11a/b/g/n. The RERUM GW will aggregate the transmitted data and forward them to the application server, after the secure connection with the RERUM MW and the application server has been successfully established.

The RERUM Gateway will be connected via Ethernet or 802.11a/b/g/n to an Internet access point, which will use cellular (GPRS) as the transmission protocols.

The application server will be an Apache Web server with PHP and Round-robin Database (RRD) implemented on it. RDs are particularly designed for handling time-series data like network bandwidth, temperatures, etc. The acquired data are stored in a circular buffer based database. The RRDtool which will be installed in the server assumes time-variable data in intervals of a certain length. This interval is specified upon creation of an RRD file and cannot be changed afterwards. Given the fact that the sensed data will be energy consumption data, this interval will be in the order of minutes (e.g., 5-10 minutes).

The application server will read the data from the and store them on the RRD. Besides the RRDtool, Cacti will also run on the application server, which will be used as a graphing tool. Cacti will allow a user to poll the monitored data at predetermined intervals and graph the resulting data. It will be used both for graphing real time-series data and data statistics.

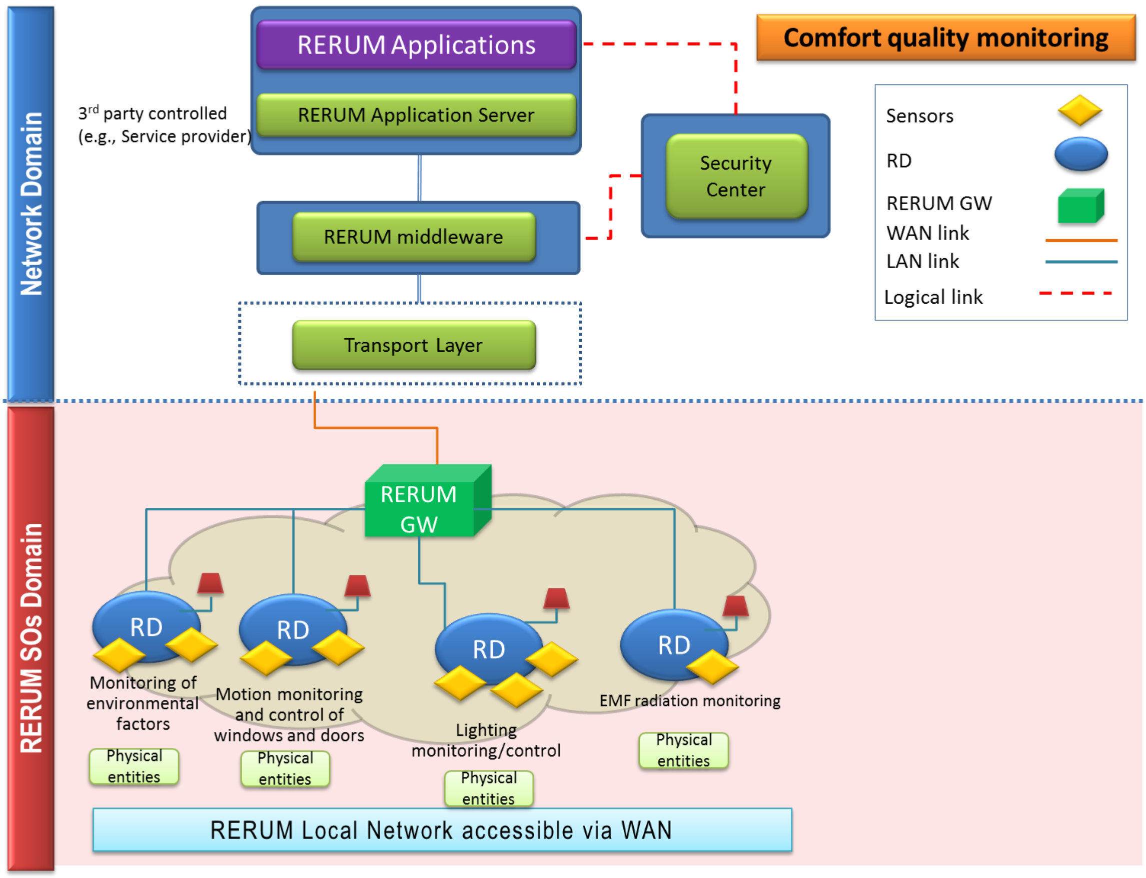

Figure 30 Comfort quality monitoring high-level overview (Heraklion)

Table 26 Interfaces between Trial components UC-I2 (Heraklion)

Components	RERUM device	Gateway	Middleware	Application Server
RERUM device	n/a	**Connectivity**: IEEE 802.11a/b/g/n IEEE 802.15.4 **Scope**: Traffic aggregation, Packet forwarding, Energy savings for devices	**n/a**	n/a
Gateway	**Connectivity**: IEEE 802.11a/b/g/n IEEE 802.15.4 **Scope**: Traffic aggregation, Packet forwarding, Energy savings for devices	n/a	**Connectivity**: Transport technology: xDSL Application layer protocol: REST based on http.	n/a
Middleware	n/a	**Connectivity**: Transport technology: xDSL Application layer protocol: REST based on http.	**n/a**	**Connectivity**: technology: irrelevant Application layer protocol: REST based on http.
Application Server	n/a	n/aa	**Connectivity**: technology: irrelevant Application layer protocol: REST based on http.	n/a

Table 27 summary of the devices measurements for UC-I2 (Comfort quality monitoring), shows the sensors and devices deployed at each location:

Table 27 summary of the devices measurements for UC-I2 (Comfort quality monitoring)

Location	Measurements			Number of components	
	Temperature	RH	Presence	RD	GW
KEP	Yes	Yes	No	5	1
Town Hall	Yes	Yes	No	10	1

Location	Measurements			Number of components	
	Temperature	RH	Presence	RD	GW
Archaeological Museum	Yes	Yes	No	20	4
One of the buildings of the city technical agency	Yes	Yes	No	10	1

4.1.2.2.4 Scenarios description

The tables below include the scenarios that will be implemented in the UC-I1 trials in Heraklion

Table 28 Scenario UC-I2$_A$

Purpose of the scenario	The purpose of the scenario is to evaluate the RERUM authorization process with reputation evaluation. This scenario will make use of the final reputation engine enriched with the feedback provided in scenario UC-I1A.
Eval. criterion ID	AL.AU.1
KPIs	Defined in the criteria
Scenario Description	Create users with different reputation ratings. Look for those cases where a given user / entity should have a reputation different to neutral Prepare a policy that does not take that reputation in consideration Try to access the system with these users and note the response Change the policy to take into account the evaluation Try to access the system with these users and note the response Check whether the access decision changes
Topology	Figure 31, Figure 32

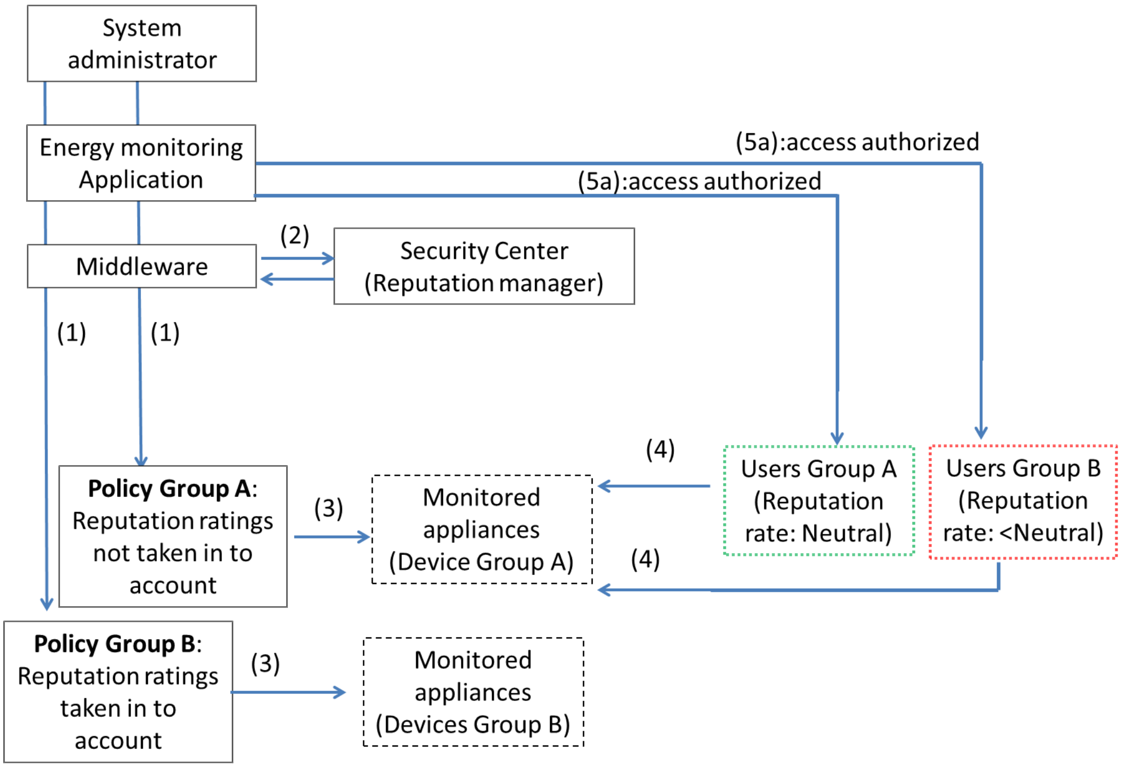

Figure 31 Scenario UC-I2$_A$ (No group policy applied)

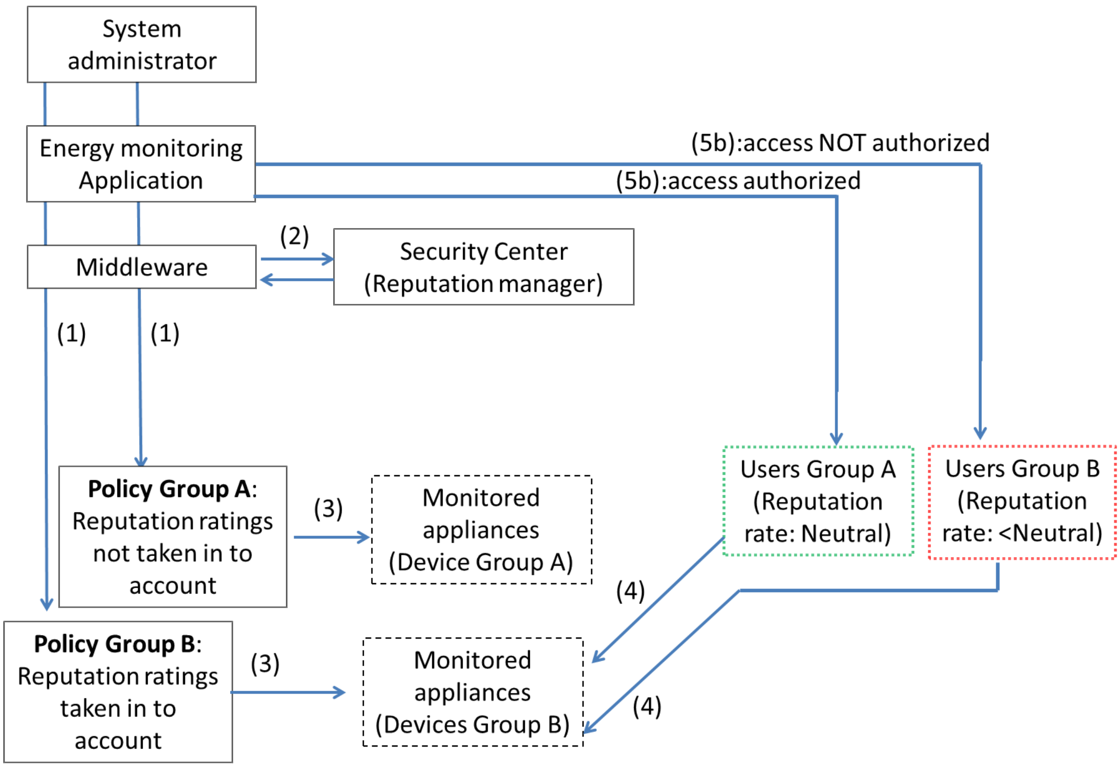

Figure 32 Scenario UC-I2$_A$ (Group policy applied)

As shown in Figure 31, the administrator can apply different policies to different group of devices in order to control the reaction of those groups to the reputation level of the end-user that also are grouped into different groups with different reputation levels. In this scenario, the reputation levels are not taken into account by the monitored devices (through the middleware and the reputation manager) and as a result end-users that belong to different groups with different reputation levels can both access the devices.

On the contrary, as shown in Figure 32, when the reputation level is set to be taken into account through the policy that applies the administrator, the end-users that belong to a group with lower reputation level that "normal" then they are expected to not be able to access the devices that belong to a group with a policy that required the reputation level to be at least "normal".

Table 29 Scenario UC-I1$_B$

Purpose of the scenario	The purpose of the scenario is to evaluate the RERUM authorization process based on user roles
Eval. criterion ID	AL.AU.2
KPIs	Success of policy control
Scenario Description	Define a user attribute role in the Identity platform or make sure that you use an already existing one in the following step For each zone of the building subject to be accessed by a different user, upload in the system 1 security policy that checks the proer role for that zone Check the policy with different users that have different values for that attribute by inspecting the logs of the authorization engine
Topology	Figure 31, Figure 32

This scenario will try to check the access of distinct users with different roles to the distinct zones of the public buildings. For each zone supposed to be accessed by different people it will be necessary to create proper policy files that allow accessing them only to those users that have the proper role associated.

4.1.2.2.5 Requirements and dependencies

No requirements or dependencies have been identified.

4.1.2.2.6 Scheduling of the activities

Table 30 Heraklion's scheduling activities for UC-I2

Date	Actions
End of January 2016	The application server will be ready. The connection between the necessary RERUM architectural components and the respective protocols' functionalities will be tested.
End of March 2016	The RDs will be deployed in the specified places and the connectivity with the application server and the RERUM architectural components will be tested.
April 2016	Trials begin to run live. The support will be continuous in order to • Assess the feedback that will be provided by Tarragona, regarding the UC-I2 trials in 1st phase. • gather the necessary information for the evaluation of the trial • face any problems that may occur

Date	Actions
	• improve any functionalities and mechanisms
July 2016	End of 2nd phase trials. Final evaluation. Cross evaluation.

4.1.2.2.7 Risks and related solutions

The possible risks for UC-I2 are the same as UC-I1.

4.2 Tarragona Trials

4.2.1 Phase-1 Trials

4.2.1.1 UC-O2: Outdoor - Environmental monitoring

4.2.1.1.1 Definition

Tarragona's goal is to gather environmental information to study its impact on their cultural assets. Most of them are World Heritage[2] monuments from the Roman period of the city. In particular the aim is to study how the environmental pollution affects to the municipality monuments, such as the contaminants which influence the water acidity (Like the sulphur dioxide, the nitrates or the carbon oxides)

Furthermore, meteorological stations will be deployed along with some of the installed devices to estimate the environmental conditions that have a direct impact to the municipality monuments. This information could be used, as well, for other purposes like internal planning or to provide information to the citizens.

Finally, to maximise the results in the devices deployment, several noise sensors will be installed as a trial pilot to advance in the city efforts on this topic.

In conclusion, the trials in the city will measure the following elements:

- Weather conditions (Temperature, RH, …)
- Air quality (SO2, NOx, O3, CO_x, VOC, PM10)
- Noise

The collected data will be forwarded to an application server, where it will be processed in order to be usable by an end-user in terms of:

- Real-time and geolocalized monitoring of environmental factors.
- Comparison of environmental information from different spots.
- Historical evolution of environmental parameters.
- Study the pollution and meteorological impact to the city monuments.
- Allow to label special environmental conditions in the city (i.e. the pollution generated by Tarragona's annual Fireworks Contest).
- Raise alerts if the environmental pollution is over a threshold.
- Allow other applications, not linked with the project, to access the collected data.

[2] http://whc.unesco.org/en/list/875

The main goals of the environmental monitoring system are the following:

- Get indicative measurements of the air quality of the city at different spots.
- Monitor both the pollution and the meteorological impact on heritage assets.
- Study the effects on the air quality when different decisions are taken from the city council in terms of mobility in the streets.
- Correlate all measures made with the existing weather on each part of the city the system is deployed.

4.2.1.1.2 Mapping of UC ecosystem components to trial functionality and technical components

Table 31 UC-O2: main components (Tarragona)

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 18 for further details on sensors used in UC-O2.
RERUM Devices	The RDs 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 RDs 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. RDs communicate wirelessly, using 6LoWPAN over IEEE 802.15.4 (on the specified frequency bands). RDs are composed of: • A RF IEEE 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 RD 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. • Noise and rain: according also to the EC directives [5], the noise could not

Component	Description
	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 RDs' wireless communication technology, it is necessary to add gateways or cluster heads close to RDs to communicate/fuse the gathered data to the application server over the internet. Thus, a gateway will be equipped with an IEEE 802.15.4 interface for communication with the RDs 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.

Table 32 UC-O2: sensor types (Tarragona)

Sensor	Sensing elements	Description	Common Uses
Weather	Temperature Relative Humidity (RH) (Others: Atmospheric pressure, rain, lux meter)	Measures the current weather conditions	Helps to interpret the air quality information
Air Quality	SO_2 NO_X O_3 VOC PM_{10}	Measures the key air compounds (mainly those related to traffic and fuel combustion)	Determine an air quality index, control the PM and relate it to the possible effects on the city assets.
Noise	Microphone	Measures the noise level with A-weighting, peak, average and daily distribution	Determine the noise in the deployment areas.

4.2.1.1.3 Deployment of components

The RDs to be installed in the city locations will transmit the sensed data to a RERUM GW that will be installed in the proximity of the RDs. The number of RERUM GWs will depend on the propagation conditions which affect the quality of the connection (e.g., bit rate, connection reliability). The transmission protocol will be 6LowPan over IEEE 802.15.4, although some devices could use 802.11a/b/g/n or Ethernet as well. The RERUM GW will aggregate the transmitted data and forward them to the application server or to another external middleware, after the secure connection with the RERUM MW and the application server has been successfully established.

In regard of the current use case high-level overview, it is not reproduced again here due its similarities to the one described before in the Heraklion's UC (please see "Figure 26 Environmental monitoring high-level overview (Heraklion)").

Table 33 UC-O2: Interfaces between Trial components (Tarragona)

Components	RD	Gateway	Middleware	Application Server
RERUM device		**Connectivity**: IEEE 802.15.4, IEEE 802.11a/b/g/n, Ethernet. **Scope**: Traffic aggregation, Packet forwarding, Energy savings for devices.		
Gateway	**Connectivity**: IEEE 802.15.4, IEEE 802.11a/b/g/n, Ethernet. **Scope**: Traffic aggregation, Packet forwarding, Energy savings for devices		**Connectivity**: Technology: GPRS, IEEE 802.11a/b/g/n, Ethernet **Scope**: Security: device authentication …	**Connectivity**: Technology: GPRS, IEEE 802.11a/b/g/n, Ethernet
Middleware		**Connectivity**: Technology: GPRS, IEEE 802.11a/b/g/n, Ethernet **Scope**: Security: device authentication …		**Connectivity:** TCP/IP (Ethernet, VNPs, xDSL) **Scope:** Gather, process and display sensor data.

Finally, with respect to the devices deployment, the RDs will be installed in several heritage assets:

- Around Tarragona's Roman Wall:
  - The Pretorium Tower.
  - Wicket gate at Sant Antoni Street.
  - Canals' Estate roof.
  - North area of the Roman Wall.
- Roman Amphitheatre.

Table 34 UC-O2: summary of the devices measurements (Tarragona)

Map Id.	Location	Measurements – sensors			Number of devices		
		Air quality	Noise	Weather	RDs	RD Power	GW

Map Id.	Location	Measurements – sensors			Number of devices		
		Air quality	Noise	Weather	RDs	RD Power	GW
1 & 5	Pretorium Tower	Yes	Yes	Yes	1-2	AC / battery	1-2*
2	Wicket gate	Yes	Yes	No	1	AC / battery	1
3	Canals Estate	Yes	Yes	No	1	AC / battery	1*
4	Roman Wall north area	Yes	No	Yes	2	AC / battery	1
6	Roman Amphitheatre	Yes	No	Yes	2	AC / battery	1

* In locations number 1 and 3 the gateway may be shared between indoor (UC-I2) and outdoor (UC-O2) use cases.

The RERUM devices will be connected using the council's internal network. In some points, if the city network is not available, other kind of connections like GPRS would be considered.

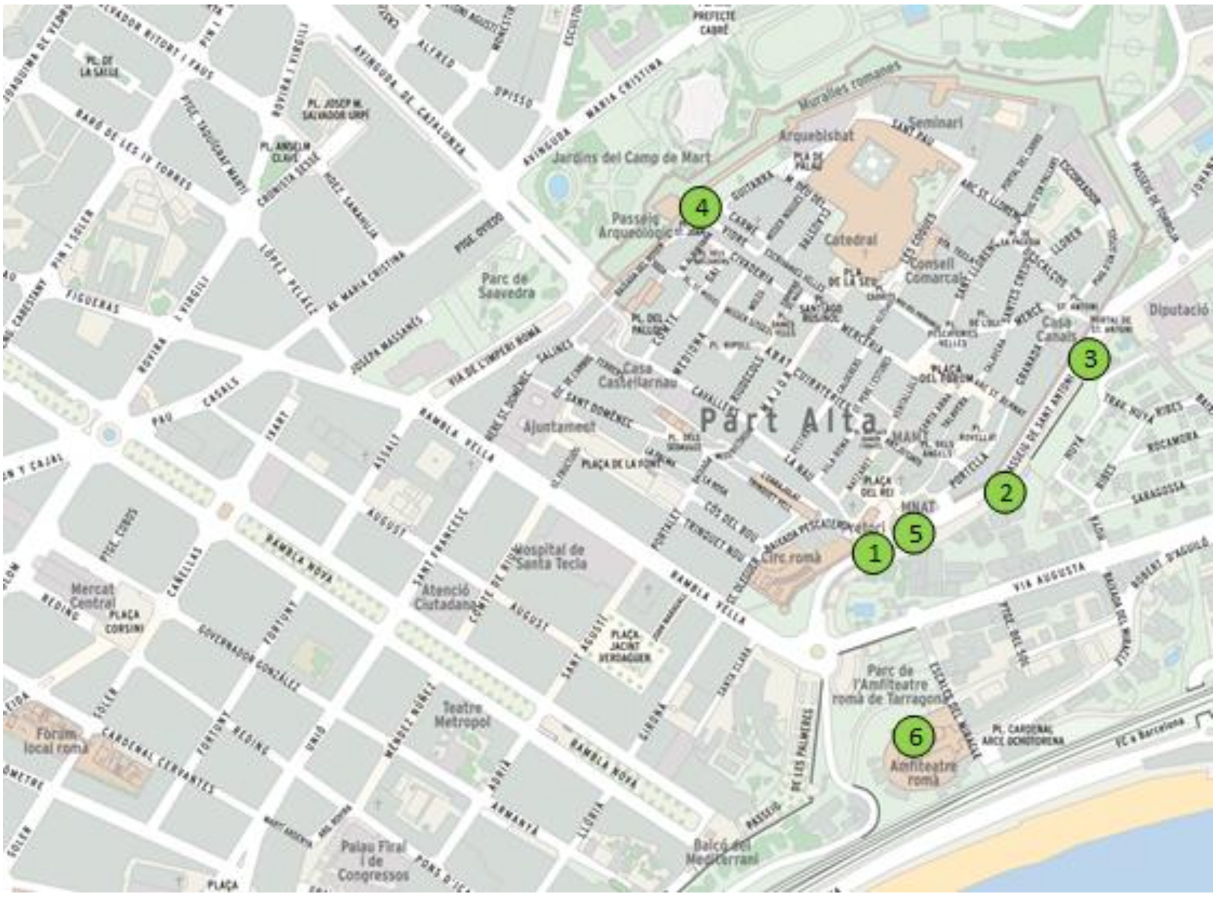

Figure 33 Placement of sensors for UC-O2 trials (Tarragona)

Figure 34 Tarragona's Pretorium tower [6]

Figure 35 Tarragona's Roman Amphitheatre

4.2.1.1.4 Scenarios description

The tables below include the scenarios that will be implemented in the UC-O2 trials in Tarragona

Table 35 Scenario T-UC-O2$_A$

Purpose of the scenario	Demonstrate how M/W functions can leverage layer 3 multicast in order to improve network performance and decrease energy consumption, ultimately increasing deployment lifetime.
Evaluation criterion ID	AL.PE.5
KPIs	All defined in the criterion
Scenario Description	To implement the evaluation defined in section 2.3.4, a message will be send from the end-user application to a selected group of RDs. The message will ask the RDs to perform a predetermined action (i.e. do a measurement, check version of currently installed firmware, or provide information about the devices like their status) and return an answer to the server.
Topology	See Figure 28

Table 36 Scenario T-UC-O2$_B$

Purpose of the scenario	Provide availability information of deployed devices to allow users and maintainers to assert the deployment status, schedule preventive maintenance if one or more devices show behaviours prone to failure, and to provide users and services exploiting the data reliability criteria.
Evaluation criterion ID	EM.PE.8
KPIs	All defined in the criterion
Scenario Description	As defined in the criterion.
Topology	The standard topology defined for this UC in Figure 26.

Table 37 Scenario T-UC-O2$_C$

Purpose of the scenario	Test the OAP in the outdoor installed RDs, which may be deployed in hard to access areas.
Evaluation criterion ID	AL.SE.2
KPIs	All defined in the criterion.
Scenario Description	The RDs will be deployed in hard to access areas. The OAP will minimise the need to send a technician to each device to reprogram them, so the system's maintenance cost should decrease.
Topology	The standard topology defined for this UC in Figure 29.

Table 38 Scenario T-UC-O2$_D$

Purpose of the scenario	Test if the ABAC authorization security is able to make access decisions based on the day or hour of the request.
Evaluation criterion ID	AL.AU.3

KPIs	All defined in the criterion.
Scenario Description	Prepare XACML policies that take into account the date and time of the request, respectively, and check they work properly by executing operations through the applications at distinct hours and days to cover the four possible combinations of date / time with available and non-available slots.
Topology	The standard topology defined for this UC in Figure 26.

4.2.1.1.5 Requirements and dependencies

Some of the RDs will be installed in heritage assets. Therefore these RDs must meet the following criteria:

- The RDs visual impact on the monument must be low or non-existent.
- The RDs must be fixed in the monuments by non-abrasive and non-permanent techniques (i.e. silicone cement or plastic clamps).

The RDs must not interfere with other wireless devices already deployed in the city.

The RDs physical deployment must be coordinated with the Council's maintenance companies. Consequently, to ease the device's installation and maintenance a procedure must be written down to determine how the different involved parties (Council employees, maintenance companies and RERUM partners) interact.

4.2.1.1.6 Scheduling of the activities

The schedule for the activities to be carried out in the first phase in Tarragona, for both use cases UC-O2 and UC-I2, is detailed in the following table:

Table 39 UC-O2: scheduling activities (Tarragona)

Month		Dates	Actions
Start	End		
M16	M24	December to August 2015	Trials planning and pilot use case implementation.
M25	M26	September to October 2015	Start of the first phase. A few RDs will be deployed in strategic points to early detect problems in their performance (data collection, networking, communication with the gateways and the middleware server). The middleware server will be deployed.
M27	M29	November to January 2016	Progressive RDs deployment. End-user application deployment. End of the RDs deployment.
M30	M30	February 2016	First phase evaluation: a report will be produced with the trials' results, the difficulties that have been encountered, suggested improvements, etc. This report will feed Heraklion's UC-O2 trials.
M35	M35	July 2016	Final evaluation. Cross evaluation. End of the second phase.

4.2.1.1.7 Risks and related solutions

Table 40 UC-O2: risks (Tarragona)

Risk description	Probability to occur	Suggested solution
As some of the RDs will be deployed within heritage assets, a written authorization from the Catalonian Government might be required. The Government may not authorise the deployment.	Low	The sensors will be reallocated outside the heritage assets.
Networking problems.	Medium	Additional gateways could be deployed. The equipment could have installed special antennas or to use GPRS for communication.
RDs are destroyed because of vandalism or stolen.	Low	RDs will be installed in points where it will be difficult the physical access.
Unforeseen difficulties in the physical deployment.	Low	Alternative locations for the sensors would be considered.

4.2.1.2 UC-I2: Indoor - Comfort quality monitoring

4.2.1.2.1 Definition

Tarragona will perform environmental monitoring inside several municipal buildings, some of them museums, in order to monitor their air quality. In particular the following items will be measured:

- Temperature.
- Relative Humidity.
- Luminance.

The collection of the three environmental indicators will allow the Council to known the building's real status and, maybe, to help to prioritize the maintenance activities in the facilities. In a key location, RERUM may allow to bring smartness to a domestic-designed air conditioning system -- which at the moment is manually operated-- activating and deactivating the appliances according to the real-time data provided by the sensors.

The collected data will be forwarded to an application server, where it will be processed in order to be usable by an end-user in terms of:

- Control in real-time the environmental conditions.
- Raise alerts if the indoor quality is over a threshold.
- Historical evolution of indoor quality parameters.
- Historical evolution of indoor quality parameters by season (summer, winter …).
- Correlate the number of visitors --information manually introduced in the application-- with the indoor quality parameters.
- Obtain reference indicators.

Other objectives of this trial are the following:

- Get indicative measurements of indoor air quality.
- Get indicative measurements of the building status.
- Help to improve the staff working conditions.
- The deployed RERUM devices must not interfere with other deployed systems.
- Look after the preventive maintenance of the facilities and the historical assets.
- (Optionally) 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.
- Use the air quality monitoring at indoor places for adjusting existing policies of the municipality

4.2.1.2.2 Mapping of UC ecosystem components to trial functionality and technical components

The main components for Tarragona's implementation of user case I1 are the same already listed in "Table 11 Heraklion's UC-I1 main components" with the following exceptions:

Table 41 UC-I2: main components (Tarragona)

Component	Description
Actuators	Optionally in one of the locations, the Castellarnau's Estate, four or five actuators could be installed to bring smartness in a domestic-designed air conditioning system. The actuators could cut the power of the appliances when the measures from the sensors are above a threshold. (and vice versa) The appliances will be dehumidifiers used to control de relative humidity (from two to four) and fans used to remove hot air pockets (from one to three).

Table 42 UC-I2: sensor types (Tarragona)

Sensor	Sensing elements	Description	Common Uses
Air Quality	Temperature Relative Hummidity	Measures the temperature and humidity.	Determine an air quality inside the buildings.
Safety and Security	Infrared	Measures the infrared radiation emitted by heat.	Determine the presence and movement of living beings.

4.2.1.2.3 Deployment of components

The devices will be installed at the following places.

- Castellarnau's Estate (Museum).
- Canals' Estate (Museum).
- Inside Roman heritage assets as the Pretorium Tower.

Table 43 UC-I2: summary of the devices measurements (Tarragona)

Location	Measurements			Number of components		
	Temperature	RH	Presence	RD	RD power	GW
Castellarnau's Estate	Yes	Yes	No	5 –10*	AC / battery**	2
Canals' Estate	Yes	Yes	No	2 – 3	AC / battery**	1***
Pretorium Tower	Yes	Yes	No	3	AC / battery**	1***

* The number of RDs includes the actuators which may be installed.
** Although it is expected to have the RDs directly plugged to an AC power source, in some locations a battery will be need to assure the devices remain operational during the night, after the AC power has been cut off.
*** For these locations the gateway may be shared between indoor (UC-I2) and outdoor (UC-O2) use cases.

The RDs to be installed in the city locations will transmit the sensed data to a RERUM GW that will be installed in the proximity of the RDs. The number of RERUM GWs will depend on the propagation conditions which affect the quality of the connection (e.g., bit rate, connection reliability). The transmission protocol will be 6LowPan over IEEE 802.15.4, although some devices could use 802.11a/b/g/n or Ethernet as well. The RERUM GW will aggregate the transmitted data and forward them to the application server or to another external middleware, after the secure connection with the RERUM MW and the application server has been successfully established.

The RERUM Gateway will be connected via Ethernet, GPRS, IEEE 802.11a/b/g/n to an Internet access point.

As for the application server, it will be an Apache Web server with PHP or a Java application over a JBoss/Tomcat. The final technology will be agreed between the involved partners in tasks 5.4 and 5.5.

In regard of the current use case high-level overview, it is not reproduced again here due its similarities to the one described before in the Heraklion's UC (please see "Figure 30 Comfort quality monitoring high-level overview (Heraklion)").

Table 44 UC-I2: Interfaces between Trial components (Tarragona)

Components	RD	Gateway	Middleware	Application Server
RERUM device		**Connectivity**: IEEE 802.15.4, IEEE 802.11a/b/g/n, Ethernet. **Scope**: Traffic aggregation, Packet forwarding, Energy savings for devices.		
Gateway	**Connectivity**: IEEE 802.15.4, IEEE 802.11a/b/g/n, Ethernet. **Scope**: Traffic aggregation, Packet forwarding, Energy savings for devices		**Connectivity**: Technology: GPRS, IEEE 802.11a/b/g/n, Ethernet **Scope**: Security: device authentication …	**Connectivity**: Technology: GPRS, IEEE 802.11a/b/g/n, Ethernet
Middleware		**Connectivity**: Technology: GPRS, IEEE 802.11a/b/g/n, Ethernet **Scope**: Security: device authentication …		**Connectivity:** TCP/IP (Ethernet, VNPs, xDSL) **Scope:** Gather, process and display sensor data.

Figure 36 Castellarnau's Estate (Tarragona)

4.2.1.2.4 Scenarios description

The tables below include the scenarios that will be implemented in the UC-I2 trials in Tarragona

Table 45 Scenario T-UC-I2$_A$

Purpose of the scenario	Evaluate the SIEM server by monitoring the RDs, both sensors and actuators, deployed in the use case.
Evaluation criterion ID	AL.SE.1
KPIs	All defined in the criterion.
Scenario Description	In one of the use case locations several actuators will be installed to turn off and on domestic-designed appliances according to the environmental data provided by the RDs sensors. The SIEM interface will monitor and analyse the events, thus ensuring the system reliability. Furthermore, if the values are over a threshold the system could raise an additional alarm.
Topology	The standard topology defined in Figure 26.

Table 46 Scenario T-UC-I2$_B$

Purpose of the scenario	Test the ABAC security authorization in IoT with specific business data contained in the attributes of the user who is issuing a request.
Evaluation criterion ID	AL.AU.2
KPIs	All in the criterion.
Scenario Description	For this scenario several ABAC security policies will be defined for different user roles, being the users from the council or from third-parties (i.e. RERUM partners). The trials will evaluate if the users are allowed to the application according their attributes.
Topology	The standard topology defined for the UC in Figure 30.

Table 47 Scenario T-UC-I2$_C$

Purpose of the scenario	Test if the ABAC security is effectively able to enforce privacy criteria based on purpose parameter.
Evaluation criterion ID	AL.AU.5
KPIs	All in the criterion.
Scenario Description	A privacy policy will be defined to ensure that the incoming requests for data contain the mandatory purpose field. The trials will evaluate if the data is accessed according to the established privacy policy.
Topology	The standard topology defined for the UC.

Table 48 Scenario T-UC-I2$_D$

Purpose of the scenario	Test if the administrator is effectively able to define and upload his own security criteria to the system in a friendly manner.
Evaluation criterion ID	AL.AU.6
KPIs	All in the criterion
Scenario Description	RERUM provides an extremely authorization engine based on XACML policies. However, XACML is a very complex language and user administrators are not prone to know it, at least at its full power. For this reason, the RERUM prototype includes an API that allows for the automatic creation of XACML policies without any XACML knowledge. The applications are meant to provide a GUI to invoke this API so an administrator can easily create the XACML policies on his own
Topology	The standard topology defined for the UC.

4.2.1.2.5 Requirements and dependencies

Some of the RDs will be installed in heritage assets. Therefore these RDs must meet the following criteria:

- The RDs visual impact on the monument must be low.
- The RDs must be fixed in the monuments by non-abrasive and non-permanent techniques (i.e. silicone cement or plastic clamps).

The RDs must not interfere with other wireless devices already deployed in the locations.

To ease the device's installation and maintenance a procedure must be written down to determine how the different involved parties (Council employees, maintenance companies and RERUM partners) interact.

4.2.1.2.6 Scheduling of the activities

As the schedule for the activities to be carried out in the first phase in Tarragona is the same, please examine "Table 39 UC-O2: scheduling activities (Tarragona)".

4.2.1.2.7 Risks and related solutions

Table 49 UC-I2: risks (Tarragona)

Risk description	Probability to occur	Suggested solution
As some of the RDs will be deployed within heritage assets, a previous written authorization from the Catalonian Government might be required. The Government may not authorise the deployment.	Low	The sensors will be reallocated outside the heritage assets.
Networking problems.	Low	Additional gateways could be deployed. The equipment could have installed special antennas or to use GPRS for communication.
Unforeseen difficulties in the physical deployment.	Low	Alternative locations for the sensors would be considered.

4.2.2 Phase-2 Trials

4.2.2.1 UC-O1: Outdoor - Smart Transportation

4.2.2.1.1 Definition

The aim of UC-O1 trials is to provide proof of concept of how RERUM technologies could be used to improve and complement the available resources for the urban mobility control and monitoring.

Tarragona already has several information sources for the urban mobility control as, for instance, the geolocalization systems installed in the city buses, mobile sensors to count the vehicles or an ATC system installed in key traffic lights, which it is expected to be operational soon.

With the field trials Tarragona wishes, firstly, to increase the available information on urban mobility and, secondly, to have a system for data visualization and interpretation. Being the data collected from both RERUM devices and, as far as practicable, the sensors already deployed within the city.

For the trials an Android crowdsourcing application will be provided to a group of volunteers --who closely cooperate with the Tarragona city Council-- and the public in general to gather the following data:

- Vehicle Type
- Location
- Speed
- Direction of travel

The collected information, from both RD and external sources, could be used for:

- Perform measurements throughout the city
- Visualize traffic measurements, in a privacy conserving manner.
- Ensure the trustworthy exchange of information between the smart objects and the applications
- Preserve the privacy of user data and ensure the trustworthy and secure transmission of user data to the applications. Always anonymise user data before transmission (at smart object level)

Furthermore, the Android applications used in the trials must fulfil the following requirements:

- Preserve the user privacy (e.g.: personal data, IP address, device unique ids, potential access to the data stored in the volunteer's device).
- Avoid harmful side effects in the volunteers' smartphones (i.e.: consumption of processing resources, energy or mobile data consumption).
- Take the necessary actions to assure that young individuals do not participate in the trials.
- Gather the informed consent from the users.
- If personal data is collected, provide a procedure to allow the users to enforce their rights to access, rectification, cancellation and objection with the gathered information.
- Meet the criteria and enforce the rights and duties defined in the Spanish Data Protection Act 15/1999 and their regulations.

4.2.2.1.2 Mapping of UC ecosystem components to trial functionality and technical components

The following table describes the main components deployed for the UC-O1.

Table 50 UC-O1: main components (Tarragona)

Component	Description	Physical installation
Vehicles	Citizen car or public transport (bus, taxi) used by volunteers The objective will be to utilize the available participatory deployed RDs in an optimum way regarding the efficiency of the traffic estimation.	Smartphones carried by volunteers Devices with sensors already installed on buses
Sensors	Sensing elements of the type described in Table 51.	
RERUM Devices	For the groups of volunteers, smartphones will be utilized as RDs. The requirements that have to be satisfied are the sensing elements of Table 51 and the network connectivity which shall include WiFi and GPRS connectivity. The connectivity of the smartphones with respect to the time they keep attached to the cellular network (PDP context) will be taken into account in order not to unnecessarily waste network resources.	Carried by volunteers
Middleware server	The MW server shall be responsible for the communication of the RDs with the application servers.	Tarragona premises
Application server	Application server shall be responsible for the transport services (e.g., traffic estimation, visualization of real-time traffic state, traffic management). They can be owned by the city or outsourced.	Tarragona premises

Table 51 Sensor types for Tarragona UC-O1, describes the sensors used in the UC-O1.

Table 51 Sensor types for Tarragona UC-O1

Sensor	Description
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.
GPS_RECEIVER	Measures the location in the WGS84 reference system as well as point speed, orientation and time.
WIFI_MODULE	Captures the MAC address and RSS of current and nearby WiFi access points.
CELLULAR_MODULE	Measures the Cell Id and RSS of current and nearby cellular base stations.

4.2.2.1.3 Deployment of components

Figure 38 below shows the overview of the architectural deployment for UC-O1.

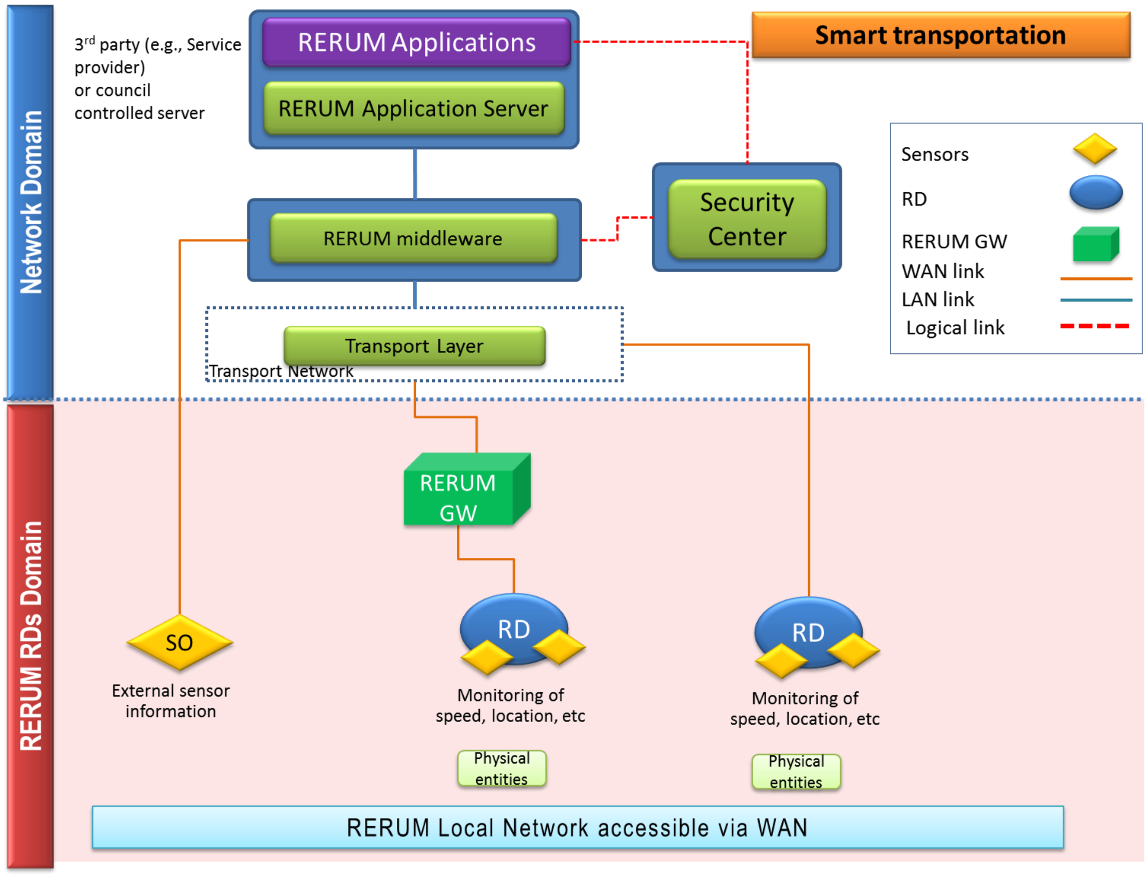

Figure 37 Tarragona UC-O1 Smart transportation high-level overview

Table 52 illustrates the interfaces between the components for UC-O1

Table 52 UC-O1 Interfaces between Trial components (Tarragona)

Components	Smartphone	Gateway	Middleware	Application Server
Smartphone			**Connectivity**: Technology: GPRS, 3G, IEEE 802.11a/b/g/n. **Scope**: Security: device authentication, traffic aggregation.	
Middleware		**Connectivity**: Technology: GPRS, 3G, IEEE 802.11a/b/g/n. **Scope**: Security: device authentication, traffic aggregation., …		**Connectivity:** TCP/IP (Ethernet, VNPs, xDSL) **Scope:** To gather, process and display sensor data.

Components	Smartphone	Gateway	Middleware	Application Server
External (non-RERUM) sensor data				**Connectivity:** TCP/IP (Ethernet, VNPs, xDSL) **Scope:** Gather and integrate external data.

As the Android application requires a minimum number of active users, the application will be distributed to a volunteer group who collaborate with the Council. If more users are required then the application will be released to other groups (i.e. students) or to the public in general.

The volunteers will be engaged in three ways:

- Specific sessions to introduce the project and the application.
- Specific actions to obtain feedback from the users (surveys or other mechanisms).
- Open a helpdesk channel to provide user support.

If the application is released to other groups a communication plan will be drawn to address them in the most effective way.

On the other hand, in spite of the external sensor data, information from Tarragona's bus company and from ATCs could be incorporated into the system. Tarragona's public transportation company currently serves 20 routes, where three of them are night routes:

Table 53 Tarragona bus routes

Route	Description
3	La Canonja – Torreforta – Tarragona
5	Prat de la Riba – St. Salvador
6	Campclar – Centre – St Pere i St Pau
8	Hosp. Joan XXIII - Camí de la Cuixa - Vall de l'Arrabassada
11	Boscos - Pl.Imp.Tàrraco
12	La Mora - Pl.Imp.Tàrraco
13	Entrepins - Sta. Tecla Llevant
21	Estació - Pg.Torroja - Catalunya - Pl.Imp.Tàrraco - Estació
22	Hospital Joan XXIII - El Serrallo
23	Estació - Hosp. Joan XXIII
30	La Canonja
34	Colom- La Floresta - Les Gavarres

Route	Description
41	Zona Educacional
42	Complex Educatiu
52	Bonavista – Pere Martell – Cooperativa Tàrraco
55	Rodolat del Moro - St. Pere i St. Pau
85	Hospital Joan XXIII – St. Salvador
71	[night route] Pl.Imp.Tàrraco - St. Pere i St. Pau - St. Salvador
72	[night route] Pl.Imp.Tàrraco - La Canonja
73	[night route] Pl.Imp.Tàrraco - Boscos

For the trials the routes which operate in the city critical areas will be chosen. This will be decided taking into consideration the feedback from the 1st phase provided by Heraklion.

4.2.2.1.4 Scenarios description

The tables below include the scenarios that will be implemented in the UC-O1 trials in Tarragona

Table 54 Scenario T-UC-O1$_A$

Purpose of the scenario	Measure the battery consumption of the developed Android application once the RERUM middleware is used with them.
Evaluation criterion ID	ST.EF.1
KPIs	The application users will answer a questionnaire evaluating if they have observed significant battery depletion after installing the RERUM application [UE.ST.1]
Scenario Description	Volunteers will use a RERUM Android application to provide mobility information. The application will be installed in their own smartphones.
Topology	The standard topology for the use case defined in Figure 38

Table 55 Scenario T-UC-O1$_B$

Purpose of the scenario	Measure the CPU load of the developed Android application once the RERUM middleware is used with them.
Evaluation criterion ID	ST.EF.2
KPIs	The application users will answer a questionnaire evaluating if the application's performance is acceptable [UE.CO.1]
Scenario Description	Volunteers will use a RERUM Android application to provide mobility information. The application will be installed in their own smartphones.
Topology	The standard topology for the use case defined in Figure 38

Table 56 Scenario T-UC-O1$_C$

Purpose of the scenario	Measure the uptime of the developed Android application once the RERUM middleware is used on them.
Evaluation criterion ID	ST.PE.1
KPIs	As defined in the criterion.
Scenario Description	The application users will answer a questionnaire evaluating if the application's performance is acceptable [UE.CO.1]
Topology	The standard topology for the use case defined in Figure 38

4.2.2.1.5 Requirements and dependencies

The RDs in this UC trial are android based smartphones that run RERUM application. Due to the vast amount of combinations of hardware and software versions available on the market for Android smartphones, using arbitrary devices it can be a difficult task within the project to assure good quality of tests in the trials. To address this issue we will provide a list of validated smartphones and their expected performance in the trials. The current list can be seen in Table 9 (Heraklion UC) and it will be continuously updated. LiU will, furthermore, provide timely validation of any device proposed by the city.

In the trials the demo application is intended to demonstrate the RERUM platform/architecture in a traffic management use case. The use case is limited to traffic estimation proof-of-concept, over the RERUM-collected data.

Collection of data is carried out with the help of vehicle-mounted devices and devices carried by citizens. There are 2 categories of users:

- Public transportation dedicated to specific routes
    - The quality of traffic estimation is directly affected by the amount of data collected.
- Participatory group of users that use smartphones
    - Users are requested to use smart-phones from the set of devices validated by LiU prior to trial and deployment.
    - The users are instructed to use only when driving their car with the help of Start-Stop button in the application.

Additionally, the Android application must be available at least in Catalan and Spanish.

4.2.2.1.6 Scheduling of the activities

The schedule for the UC-O1 in Tarragona is as it follows below.

Table 57 UC-O1: scheduling activities (Tarragona)

Month		Dates	Actions
Start	End		

<table>
<tr><th colspan="2">Month</th><th rowspan="2">Dates</th><th rowspan="2">Actions</th></tr>
<tr><th>Start</th><th>End</th></tr>
<tr><td>M28</td><td>M30</td><td>December to
February 2016</td><td>Plan and schedule the tasks. At least the following tasks should be scheduled for the second phase:
– Engage the volunteers.
– Risk assessment for the volunteers (number of users, …)
– Address the ethical aspects of the trials.
– Deploy the Android application.
– Deploy the end-user application.
Adapt the RERUM middleware for the second phase.</td></tr>
<tr><td>M30</td><td>M30</td><td>February 2016</td><td>Use Heraklion’s early results to improve the planning and schedule.</td></tr>
<tr><td>M31</td><td>M35</td><td>March to July 2016</td><td>Second phase start.
Volunteer engagement and RD deployment.
End-user application deployment.</td></tr>
<tr><td>M35</td><td>M35</td><td>July 2016</td><td>Final evaluation. Cross evaluation.
End of the second phase.</td></tr>
</table>

4.2.2.1.7 Risks and related solutions

The foreseen risks in UC-O1 in Tarragona are described in Table 58:

Table 58 UC-O1: risks (Tarragona)

<table>
<tr><th>Risk description</th><th>Probability to occur</th><th>Suggested solution</th></tr>
<tr><td>Low participation: Quality is directly proportional to data collected. The number of active users is too low for the trials’ requirements.</td><td>Medium</td><td>Communication and training actions will take place to increase the number of active users.
As an alternative, the application will be distributed among other groups or volunteers or to the public in general though an open call.</td></tr>
<tr><td>Proper operation of the application: Proper training for the user to understand when the application starts and stops.</td><td>Medium</td><td rowspan="2">Communication and training actions will take place to increase the number of active users.</td></tr>
<tr><td>Collection of unnecessary data: Stop application when the user is out of the vehicle.</td><td>Medium</td></tr>
<tr><td>Participant tries to use an unsupported Android smartphone. The application malfunctions (poor GUI, non-responsive, crash)</td><td>Medium</td><td>The list of tested phones on Table 9 is constantly expanded, covering a significant portion of commonly available devices. However some the user may not be able to participate in the trial. In case this number is excessive among the volunteers and there is a limited number of devices we will attempt to update the app</td></tr>
</table>

4.2.2.2 UC-I1: Indoor - Home energy management

4.2.2.2.1 Definition

The goal of UC-I1 trials is to monitor the energy consumption in some of the Council's office buildings. The monitoring goals will be the following to detect abnormal readings (e.g. appliances or lights turned on in a weekend) and to study the patterns of energy consumption according to the season (e.g. use of air conditioning). The monitor will focus on the following:

- Energy consumption of air conditioners (A/C)s
- Energy consumption of personal computers (PCs) and other appliances.
- Energy consumption of lighting

The collected data will be forwarded to an application server, where they will be processed in order to be usable by an end-user (e.g., building administrator) in terms of:

- Real-time energy monitoring of requested device(s).
- Extraction of statistical results for the energy consumption of the devices.

Other objectives of this trial are the following:

- Identify relationships between environmental factors and energy consumption
- Raise alarms when the measurements show abnormal consumption behaviour or excessive use above pre-defined thresholds.
- Ensure the reliable operation of the system
- Ensure the trustworthy exchange of information between the smart objects and the foreseen smart city applications
- Preserve the privacy and non-disclosure of the home-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)
- Support the "always connected" nature of the indoor smart objects
- Secure the network and avoid attacks, such as jamming, passive listening, data falsification, etc.
- Automatic secure configuration of smart objects
- Avoid network failures

4.2.2.2.2 Mapping of UC ecosystem components to trial functionality and technical components

Table 59 UC-I1: main components (Tarragona)

Component	Description
RERUM Devices	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.
Actuators	The application should raise alerts when a value is over a pre-defined threshold (i.e. lightening electrical power consumption in a weekend.)
Gateway	It will serve 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).

Component	Description
Application server	It is responsible for the end-user services. It will provide a GUI to allow the user to monitor and analyse the data collected by the sensors.

4.2.2.2.3 Deployment of components

The devices will be installed in one of the Council's office building located in Rambla Nova 59.

The RDs will be equipped with the corresponding sensors in order to monitor:

Table 60 UC-I1 summary of the devices measurements (Tarragona)

Location	Measurements				Number of components		
	Consumption	Temperature	RH	Presence	RD	RD power	GW
Rambla Nova 59	Yes	Maybe*	Maybe*	Maybe*	5 –10*	AC	1-3*

*The types of sensors and the final number of devices will be determined according the available resources after the first phase.

The RDs will transmit the sensed data to a RERUM GW, which will be deployed within the buildings. The number of RERUM GWs will depend on the indoor propagation conditions which affect the quality of the connection (e.g., bit rate, connection reliability). The transmission protocol will be 6LowPan over IEEE 802.15.4 or 802.11a/b/g/n. The RERUM GW will aggregate the transmitted data and forward them to the application server, after the secure connection with the RERUM MW and the application server has been successfully established.

The RERUM Gateway will be connected via Ethernet or 802.11a/b/g/n to an Internet access point.

As for the application server, it will be an Apache Web server with PHP or a Java application over a JBoss/Tomcat. The final technology will be agreed between the involved partners in tasks 5.4 and 5.5.

In regard of the current use case high-level overview, it is not reproduced again here due its similarities to the one described before in the Heraklion's UC (please see "Table 11 Heraklion's UC-I1 main components").

Table 61 UC-I1: Interfaces between Trial components (Tarragona)

Components	RD	Gateway	Middleware	Application Server
RERUM device		**Connectivity**: IEEE 802.15.4, IEEE 802.11a/b/g/n, Ethernet. **Scope**: Traffic aggregation, Packet forwarding, Energy savings for devices.		

Components	RD	Gateway	Middleware	Application Server
Gateway	**Connectivity**: IEEE 802.15.4, IEEE 802.11a/b/g/n, Ethernet. **Scope**: Traffic aggregation, Packet forwarding, Energy savings for devices		**Connectivity**: Technology: GPRS, IEEE 802.11a/b/g/n, Ethernet **Scope**: Security: device authentication …	**Connectivity**: Technology: GPRS, IEEE 802.11a/b/g/n, Ethernet
Middleware		**Connectivity**: Technology: GPRS, IEEE 802.11a/b/g/n, Ethernet **Scope**: Security: device authentication …		**Connectivity:** TCP/IP (Ethernet, VNPs, xDSL) **Scope:** Gather, process and display sensor data.

Figure 38 Tarragona's Council offices in Rambla Nova 59

4.2.2.2.4 Scenarios description

The tables below include the scenarios that will be implemented in the UC-I1 trials in Tarragona

Table 62 Scenario T-UC-I1$_A$

Purpose of the scenario	Demonstrate how M/W functions can leverage layer 3 multicast in order to improve network performance and decrease energy consumption, ultimately increasing deployment lifetime.
Evaluation criterion ID	AL.PE.5
KPIs	All defined in the criterion
Scenario Description	To implement the evaluation defined in section 2.3.4, a message will be send from the end-user application to a selected group of RDs. The message will ask the RDs to perform a predetermined action (i.e. take a measurement) and return an answer to the server.
Topology	See Figure 28

Table 63 Scenario T-UC-I1$_B$

Purpose of the scenario	Test the integration of ABAC authorization in IoT with specific business data contained in the attributes of the user that is issuing the request
Evaluation criterion ID	AL.AU.2
KPIs	All defined in the criterion.
Scenario Description	Use a set of previously known users to check if the predefined security policies allow or deny the access to specific data.
Topology	The standard topology defined for this UC in Figure 19

4.2.2.2.5 Requirements and dependencies

As some of the sensors may be installed inside electrical panels, the power must be cut in order to physically install them. Therefore the installation should be carefully planned to avoid service interruptions to the council stall.

Like the previous use cases in Tarragona, to ease the device's installation and maintenance a procedure must be written down to determine how the different involved parties (Council employees, maintenance companies and RERUM partners) interact.

4.2.2.2.6 Scheduling of the activities

Table 64 UC-I1 scheduling activities (Tarragona)

Month		Dates	Actions
Start	End		

Month		Dates	Actions
Start	End		
M28	M30	December to February 2016	Plan and schedule the tasks. Adapt the RERUM middleware for the second phase.
M30	M30	February 2016	Use Heraklion's early results to improve the planning and schedule.
M31	M35	March to July 2016	Second phase start. RD deployment. End-user application deployment.
M35	M35	July 2016	Final evaluation. Cross evaluation. End of the second phase.

4.2.2.2.7 Risks and related solutions

The foreseen risks for this use case are given in Table 65.

Table 65 UC-I1: risks (Tarragona)

Possible risk	Probability to occur	Suggested solution
Granularity level for RDs installation (e.g., installation on personal appliances) not accepted by building administration	Low	Granularity level for RDs installation will gradually change, e.g., from individual devices to rooms, or floors, etc. in order to reach an agreement with the building administration.
Unforeseen difficulties in the physical deployment.	Low	Alternative locations for the sensors would be considered. In the worst scenario, the user case could be implemented in another office building.

4.3 Trials ethic assessment

This section provides the replies to the ethical questions raised in section *B4.2 Requirements and Implementation of Ethics Review Report* of the REUM Description of Work document that have some implications on the trials. There is a table for each of the use cases.

4.3.1 UC-O1: Outdoor - Smart Transportation

The actions described for the Tarragona trial mitigate the ethics issues through the application of the legal measures foreseen in the Spanish regulations or through technical solutions to mitigate those risks. For the Heraklion trials, as there are no final users involved because the devices that will collect information will be installed on public buses, there are no ethical issues to consider.

Table 66 Ethics assesment for UC-O1 Smart transportation

Ethics issue	Actions taken in Tarragona trials	Actions taken in Heraklion trials
Identification of any personal data acquired, processed and stored of personal data (privacy and data protection management).	In the UC an Android Application will be distributed among volunteers. The application might collect personal data. Although the aim is to avoid collecting personal data, if personal information is gathered the following actions will be executed before the Android application distribution: − The collected personal data will be identified and classified according the Spanish Data Protection Act 15/1999. − Proper technical measures to protect the personal data will be implemented. − The persons --natural or legal-- in charge of the data will be identified. − The collected data will be explicitly described in the user consent. − The purpose of the data collection will be explicitly described in the user consent. − The parties with access to personal data will be explicitly described in the user consent. − No personal data will be transmitted to third parties. − The user will have the access, rectification, cancellation and objection rights for their personal data, and can revoke its consent and request the deletion of data regarding	The smartphones will be installed on public buses and no personal data will be used or stored. Only the location of buses will be tracked.

Ethics issue	Actions taken in Tarragona trials	Actions taken in Heraklion trials
	him/her. − The staff in charge of the data collection, storage, analysis and curation will be trained in privacy and data protection management.	
Not allow tracing of individuals in real time. Copies of approval form national data protection authorities submitted to the EC if collected data will be marked as identified or identifiable.	In the UC an Android Application will be distributed among volunteers. The application might allow to trace an individual in real-time. Obfuscation techniques will be implemented to remove the possibility of tracing users in real time.	Tracing of individuals will not happen.
Detailed information must be provided on the procedures that will be used for the recruitment of participants. Inform the participants on the procedures and personal or sensitive information gathered.	To use the application the volunteers will have to read and accept the informed consent. The volunteers will be over 18 years old. If the application is released to the public, proper measures will be implemented to assure that young people do not use the application (i.e. rate the application for 18+, explicit warning in the application …).	The smartphones will be installed on public buses and no personal data will be used or stored. Nevertheless, the bus drivers and the citizens will be aware that the buses have those devices installed on them.
Informed consent from participating volunteers.	See above.	No participating volunteers are foreseen for this use case.
Confirm that children will not be included as participants in the study	See above.	See above.
Provide a detailed description of security measures that will be implemented to prevent improper use, improper data disclosure scenarios and 'mission creep'	Obfuscation techniques will be implemented to: a) Remove the possibility of tracing users in real time and, b) Avoid as far as practicable the collection of personal data. In case of collecting personal information, it will be analysed according the Spanish Data Protection Act 15/1999 and their regulations to implement the necessary technical measures to prevent their disclosure or misuse and enforce the user's rights.	See above.

4.3.2 UC-O2: Outdoor - Environmental monitoring

As in this use case there is no possibility to collect any kind of personal information there are no specific measures to be applied as described.

Table 67 Ethics assesment for UC-O2 Environmental monitoring

Ethics issue	Actions taken in Tarragona trials	Actions taken in Heraklion trials
Identification of any personal data acquired, processed and stored of personal data (privacy and data protection management).	In the UC environmental and noise information will be measured. As the environmental information is not linked to a natural person, personal information is not going to be collected. In regard to the noise data, the deployed RDs measures noise levels, but no sound is recorded. Therefore no personal data is going to be gathered.	
Not allow tracing of individuals in real time. Copies of approval form national data protection authorities submitted to the EC if collected data will be marked as identified or identifiable.	N/A	
Detailed information must be provided on the procedures that will be used for the recruitment of participants. Inform the participants on the procedures and personal or sensitive information gathered.	N/A	
Informed consent from participating volunteers.	N/A	
Confirm that children will not be included as participants in the study	N/A	
Provide a detailed description of security measures that will be implemented to prevent improper use, improper data disclosure scenarios and 'mission creep'	N/A	

4.3.3 UC-I1: Indoor - Home energy management

In both cities the UC will be deployed in public buildings monitoring the overall energy consumption of some specific components as lighting or air conditioning, so it is not possible to monitor the behaviour of any individual based on the monitoring of energy consumption.

Table 68 Ethics assesment for UC-I1 Home energy management

Ethics issue	Actions taken in Tarragona trials	Actions taken in Heraklion trials
Identification of any personal data acquired, processed and stored of personal data (privacy	In the UC information about power consumption and human presence in a public building will be collected.	

Ethics issue	Actions taken in Tarragona trials	Actions taken in Heraklion trials
and data protection management).	As the information could not be linked to an individual, no personal data is going to be collected.	
Not allow tracing of individuals in real time. Copies of approval form national data protection authorities submitted to the EC if collected data will be marked as identified or identifiable.	N/A	
Detailed information must be provided on the procedures that will be used for the recruitment of participants. Inform the participants on the procedures and personal or sensitive information gathered.	N/A	
Informed consent from participating volunteers.	N/A	
Confirm that children will not be included as participants in the study	N/A	
Provide a detailed description of security measures that will be implemented to prevent improper use, improper data disclosure scenarios and 'mission creep'	N/A	

4.3.4 UC-I2: Indoor - Comfort quality monitoring

In both cities the UC will be deployed in public buildings monitoring the indoor environmental parameters, so it is not possible to monitor the behaviour of any individual based on the monitoring of energy consumption.

Table 69 Ethics assesment for UC-I2 Comfort quality management

Ethics issue	Actions taken in Tarragona trials	Actions taken in Heraklion trials
Identification of any personal data acquired, processed and stored of personal data (privacy and data protection management).	In the UC information about environmental conditions in public buildings will be collected. As the information could not be linked to an individual, personal data is not going to be collected.	
Not allow tracing of individuals in real time. Copies of approval form national data protection authorities submitted to the EC if collected data will be marked as identified or identifiable.	N/A	

Ethics issue	Actions taken in Tarragona trials	Actions taken in Heraklion trials
Detailed information must be provided on the procedures that will be used for the recruitment of participants. Inform the participants on the procedures and personal or sensitive information gathered.	N/A	
Informed consent from participating volunteers.	N/A	
Confirm that children will not be included as participants in the study	N/A	
Provide a detailed description of security measures that will be implemented to prevent improper use, improper data disclosure scenarios and 'mission creep'	N/A	

4.4 Trials end users survey collaboration

In order to gauge the opinions of citizens and end-users RERUM currently co-operates with the Bavarian research cluster FORSEC[3] in the areas of IoT Security (MSc. Tobias Marktscheffel, UNI PASSAU) and Security Awareness (Dr. rer. nat. Zinaida Benenson, FAU Erlangen, Germany). Mr. Marktscheffel works in the IT Security group of Prof. Posegga of the University of Passau (UNI PASSAU in RERUM) on secure service execution platforms for the Internet-of-Things. Dr. Benenson leads the Human Factors in Security and Privacy Group at the Chair of IT-Security Infrastructures (Prof. Felix Freiling). Among other things, her group successfully evaluated usability and user acceptance of anonymous credentials in two rounds of a user trial in the ABC4Trust project (https://abc4trust.eu) [7].

The currently planned co-operation is to investigate user acceptance of the IoT-enabled SmartCity use case involving participatory sensing in public transportation (UC-O1). The planned evaluation of one of the two trial rounds consists of two parts:

[3] FORSEC is a Bavarian research association that spans eight professors from five different Bavarian research institutions. Involved in FORSEC are: four universities with faculties and departments of different scope (Faculty of Economics and Business Administration at University Regensburg, Faculty of Computer Science and Mathematics at University Passau, Faculty of Computer Science at TU Munich, Technical Faculty at FAU University Erlangen-Nürnberg), and - indirectly - the Institute of Applied and Integrated Security (AISEC) at the Fraunhofer Institute in Garching.

More information about FORSEC and the two projects can be found here: https://www.bayforsec.de/en/subprojects/cluster-ii/.

1. Pre-questionnaire: The prospective end-users will be asked about their perceptions of the usefulness of the UC-O1 application, their understanding of the corresponding technology and their possible security and privacy concerns.
2. Post-questionnaire: The end-users will be asked about their perceptions of the usefulness and usability of the experienced application, understanding of the corresponding technology, their perceptions of security and privacy protection during the usage, and their intention to use this application in the future.

The results of this research would provide the FORSEC IoT team with the user requirements information for development of the IoT execution environment, whereas the FORSEC Security Awareness team would gain valuable insights into the factors of user acceptance in a real-world Smart City scenario and provide design and policy guidelines for the future Smart City development. As a result of this exercise the RERUM participants would gain insight into the user acceptance of the proposed technology and solution through the UC-O1 trials. Evaluation results of the first round would facilitate improvements for the second round.

5 Proof of concept testing scope

Checklist of testing scope of RERUM technical contributions, from D2.1 [3] that will be tested in the lab experiments and in field trials.

Table 70 Testing scope of technical contributions

Requirement to test	Lab experiment and/or trial	Type of test
Contribution 8: Energy efficiency for RDs with multiple air-interfaces	Lab experiment: 3.11, Energy Efficiency of Android-based RDs	Efficiency
Contribution 9: Enrich authorization process with reputation evaluation	Trials	Authorization
Contribution 10: Integration of ABAC in IoT with specific business data contained in the request	Trials	Authorization
Contribution 11: SIEM in a generic IoT platform	Trials	Security
Contribution 12: Incorporating adaptability to an IoT platform using PRRS and OAP	Trials	Security
Contribution 13: Malleable Signatures for controllably reduced Integrity protection	Lab experiments: 3.1, Runtime-, Memory-, Communication-Overhead of Signing and Verifying Message Payload with ECC Standard Signatures in RDs 3.2, Runtime-, Memory-, Communication-Overhead of Signing, Verifying and Messages with Malleable Signatures in RDs 3.3, Energy Efficiency of Malleable Signatures on RDs 3.4, Energy Efficiency of ECC based payload Signatures on RDs	Performance, Efficiency
Contribution 14: RSSI-based CS encryption keys	Lab experiment: 3.5, RSSI-based CS encryption keys	Performance
Contribution 15: Adaptive CS-based data gathering	Lab experiment: 3.6, Adaptive CS-based data gathering	Efficiency
Contribution 17: Android-based multi sensing application	Lab experiments: 3.10, Android-based RDs applications & services stability and accuracy 3.12, Android pilot devices measurements precision	Performance, Efficiency

Requirement to test	Lab experiment and/or trial	Type of test
Contribution 18: Framework for spectrum occupancy measurements	Trial UC-O1 Smart Transportation Lab experiment: 3.10, Android-based RDs applications & services stability and accuracy	Performance
Contribution 19: Lightweight spectrum assignment framework	Lab experiment: 3.8, Lightweight spectrum sensing and spectrum assignment framework	Performance
Contribution 21: Lightweight Datagram Transport Layer Security (DTLS) Protocol	Lab experiments: 3.14, Lightweight Datagram Transport Layer Security (DTLS) Protocol	Performance, Efficiency
Contribution 22: 6LoWPAN Multicast	Trials & Lab experiment: 3.13, 6LoWPAN Multicast	Performance
Contribution 23: Low participatory RD energy and computational consumption	Lab experiment: 3.11, Energy Efficiency of Android-based RDs	Efficiency

6 Conclusions

This deliverable describes the tests to perform on the RERUM architectural framework, through in-lab experiments that will test individual system modules, identifying potential issues for the tests to be performed during live trials through the different Use Cases application in two smart city pilots. These tests will quantifiably assess the evaluation criteria defined. A total of 24 evaluation criteria have been defined for the authorization, efficiency, performance and security criteria, most of them tested by the in-lab experiments and some others in the trials.

The in-lab tests described in section 3 will be performed in task 5.3 to assess the components developed within WP2-WP4. A total of 14 in-lab experiments have been defined, that will address and evaluate the criteria assigned to be tested in controlled lab experiments. The results from those lab experiments will enhance the components that will be integrated in task 5.2 for the trials performed in two cities, in task 5.4 for Heraklion and in in task 5.5 for Tarragona. The trials will evaluate the criteria defined to be tested in the live environments of the cities under some specific use case scenarios.

Through the use cases deployment and trials, the cities will explore the potential of the RERUM architectural framework in terms of future scenarios were the privacy characteristics an low power consumption may allow innovative projects that will take advantage of those characteristics of the RERUM architectural framework.

Some examples of future innovative deployments may be based on mixed scenarios where an application may access data from some sensors located at citizen's homes, or were an application deployed at the citizens' homes will be able to get information for external sensors to regulate through actuators internal parameters of the houses. These scenarios will keep the privacy of the users taking advantage of the characteristics of the framework that allow the non-disclosure of personal data to third parties, and therefore ensuring the privacy of the users.

The potential also extend to those scenarios where sensors and devices are located in some remote spots were the availability of continuous power is difficult to be guaranteed. Thanks to the low power consumption those devices can be powered through some alternative systems like solar panels with a battery attached, guaranteeing the operation through the whole day.

References

[1] A. Fragkiadakis, P. Charalampidis and E. Tragos, “Adaptive compressive sensing for energy efficient smart objects in IoT applications,” *Proc. of VITAE 2014,* pp. 1-5, 2014.

[2] ISO, ISO/IEC 25000:2005. "Software Engineering -- Software product Quality Requirements and Evaluation (SQuaRE)", 2005.

[3] ISO, ISO 9126-1. "Software engineering - Product quality - Part 1: Quality model", June 2001.

[4] ISO, ISO 14598-1. "Information technology - Software product evaluation - Part 1: General overview", April 1999.

[5] P. prlpz., *Pretorium tower,* Tarragona: Wikimedia Commons. This file is licensed under the Creative Commons Attribution-Share Alike 3.0 Spain license.

[6] T. Mouroutis and A. Lioumpas, “RERUM Deliverable D2.1, Use-cases definition and threat analysis,” December 2014.

[7] Y. Stamatiou, Z. Benenson, A. Girard, I. Krontiris, V. Liagkou, A. Pyrgelis and W. Tesfay, in *Course evaluation in higher education: the Patras pilot of ABC4Trust. In Attribute-based Credentials for Trust*, Springer, 2015, pp. 197-239.

[8] European Parliament and Council, “The Environmental Noise Directive (2002/49/EC),” [Online]. Available: http://ec.europa.eu/environment/noise/directive.htm.

Annex A Form to collect trials' issues

Form to collect trials' deployment and execution issues during first phase to be early exchanged with the other city for phase 2 trials.

City	<Heraklion or Tarragona>	Use case	<use case name>
Date	<date when issue occurred>	Trial phase	<1 or 2>
Reported by	<name of person reporting and affiliation>		
Name	<Short description of the issue>		
Type of issue	<Deployment / Trial execution>		
Classification	<functional / app server / middleware / hardware devices / communication / integration>		
Issue description	<Description of the issue found>		
Actions taken	<Actions taken to solve / overcome this issue>		
Final result	<Final result of the issue after taking the previous actions>		
Recommendation	<Recommendation to solve / overcome this issue in next trials>		