D3.3.3

Validation Protocol and Schedule for Smart Power Grid and Healthcare Use Cases

Project number:	257243
Project acronym:	TClouds
Project title:	Trustworthy Clouds - Privacy and Resilience for Internet-scale Critical Infrastructure
Start date of the project:	1st October, 2010
Duration:	36 months
Programme:	FP7 IP

Deliverable type:	Report
Deliverable reference number:	ICT-257243 / D3.3.3 / 2.0
Activity and Work package contributing to the deliverable:	Activity A3 / WP 3.3
Due date:	April 2013 – M31
Actual submission date:	8th May, 2013

Responsible organisation:	FCSR
Editor:	Marco Abitabile
Dissemination level:	Public
Revision:	2.0

Abstract:	In this document is described our approach to the validation process for TClouds Project and a draft of the validation activities that will be held in Y3 concerting A2 components, and A3 use cases. This document is the resubmission of D3.3.3
Keywords:	Validation protocol, requirements, validation activities

Editor

Marco Abitabile (FCSR)

Contributors

Nuno Emanuel Pereira, Miguel Areias (EDP)

Paulo Jorge Santos (EFACEC ENG)

Kees Wouters, Yvon Peters (PHI)

Disclaimer

This work was partially supported by the European Commission through the FP7-ICT program under project TClouds, number 257243.

The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose.

The user thereof uses the information at its sole risk and liability. The opinions expressed in this deliverable are those of the authors. They do not necessarily represent the views of all TClouds partners.

Executive Summary

This document represents the rewrite of deliverable D3.3.3 (after the rejection of D3.3.3 during the second review meeting).

The content of this document has been totally rewritten, while maintaining the same validation strategy as described in Chapter 2.

By reading the document the strict relation with Deliverable 2.4.2 can be noticed: the requirements described in the old D3.3.3 (often too low level and difficult to read into the overall TClouds objective) have been mapped into the higher-level requirements of D2.4.2. All the different tasks of the Validation process are based on satisfying these requirements. The validation Activities of old D3.3.3 have been consolidated into the Validation Activities of this document.

Chapter 1 is the introduction of the document, contextualizing it within the A3 activity and WP3.3. Chapter 2 (Evaluation and Validation Strategy) contains the description of the whole validation strategy with the rationale and the examples to build the overall Validation process.

Chapter 3 (Implementation of the validation strategy) consists in the actual implementation of the Validation process as described in the previous chapter. Here is also highlighted the relation of the old D3.3.3 and D2.4.2. Moreover, the chapter describes how the reviewer's requests have been addressed by providing input from the external stakeholders via tailored surveys. In the following subchapters all the four tasks consisting the Validation Process are described. At the end of the chapter are defined a draft of the validation activities that will be performed during Y3 in synergy with A2 partners.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Chapter Authors:

Marco Abitabile (FCSR)

1.1 TClouds – Trustworthy Clouds

TClouds aims to develop trustworthy Internet-scale cloud services, providing computing, network, and storage resources over the Internet. Existing cloud computing services today are generally not trusted for running critical infrastructure, which may range from business-critical tasks of large companies to mission-critical tasks for the society as a whole. The latter includes water, electricity, fuel, and food supply chains. TClouds focuses on power grids, electricity management and patient-centric health-care systems as main applications.

The TClouds project identifies and addresses legal implications and business opportunities of using infrastructure clouds, assesses security, privacy, and resilience aspects of cloud computing and contributes to building a regulatory framework enabling resilient and privacy-enhanced cloud infrastructure.

The main body of work in TClouds defines an architecture and prototype systems for securing infrastructure clouds, by providing security enhancements that can be deployed on top of commodity infrastructure clouds (as a cloud-of-clouds) and by assessing the resilience, privacy, and security extensions of existing clouds.

Furthermore, TClouds provides resilient middleware for adaptive security using a cloud-of-clouds, which is not dependent on any single cloud provider. This feature of the TClouds platform will provide tolerance and adaptability to mitigate security incidents and unstable operating conditions for a range of applications running on a cloud-of-clouds.

1.2 Benchmark Applications & User-centric Evaluation

Activity 3 focuses on the applications and the evaluation of the TClouds platform. The activity's objective is to define and validate cloud applications' architecture and specifications (the medical and the Smart Lighting System use case). For this purpose, Activity 3 will specify cloud and application functionalities and requirements, define application prototypes to be implemented on the cloud platform, and validate the application prototypes and the TClouds platform. For this purpose, the requirements defined in Activity 1 will serve as a generic guideline, which will be refined and consolidated in Activity 3. Finally, there is a continuous and close interaction between Activity 3 and Activity 2 in order to make sure that the platform and applications match the specifications and that the TClouds project achieves its overall objectives.

1.3 Work Package 3.3 – Validation and Evaluation of the TClouds platform

WP3.3 main purpose is the definition of the validation and evaluation of the TCLOUDS Platform. The idea is to make use of the results produced by WP3.1 and WP3.2 to benchmark and quantify the innovations provided by the technical work-packages of A2. To evaluate the project results, WP3.3 will first of all define the main project dimensions that need to be evaluated and the specific strategies and activities for the validation of these dimensions. After this phase it will define qualitative and, when possible, quantitative metrics and indicators, organizing the activities needed to compute these metrics. Finally it will implement the validation activities and draw conclusions on the TCLOUDS results.

1.4 Deliverable 3.3.3 – Validation protocol and schedule for Use Cases

1.4.1 Overview

The aim of Task 3.3 is to validate and evaluate the TCLOUDS platform. As part of a proper research and development cycle and part of quality control, an evaluation and validation component is necessary. It ensures that the requirements specified are met and that problems, defects and malfunctions are prevented. Although much of this should already occur in an iterative fashion throughout implementation of the requirements, a more formal point in time allows careful planning and targeted efforts.

Validation is most efficient and useful when there is a prioritization of requirements and a detailing of how the validation should occur. This detailing is most informative in a structured plan where requirements are matched to procedures that result in relevant outcomes.

Activity 3 within TCLOUDS has as its focus the evaluation of the TCOULDS platform, as well as developing applications to run on this platform. Two scenarios have been selected to serve for this purpose: a Home Healthcare case and a Smart Lighting System use case. A3 links with A1 as it uses the requirements generated there as general guidelines to adhere to. It further links to A2 as it ensures alignment of the applications to the general objectives of TCLOUDS.

This document describes the evaluation and validation strategy for the TClouds Project. The strategy outlines a process of putting forth the most important requirements, to quantify them or at least operationalize them, and to delineate criteria for success

1.4.2 Structure

Chapter 1 is the introduction of the document, contextualizing it within the A3 activity and WP3.3. Chapter 2 (Evaluation and Validation Strategy) contains the description of the whole validation strategy with the rationale and the examples to build the overall Validation process.

Chapter 3 (Implementation of the validation strategy) consists in the actual implementation of the Validation process as described in the previous chapter. Here are also highlighted the relation of the old D3.3.3 and D2.4.2. Moreover, the chapter describes how the reviewer’s requests have been addressed by providing input from the external stakeholders via tailored surveys. In the following subchapters all the four tasks consisting the Validation Process are described. At the end of the chapter a draft of the validation activities that will be performed during Y3 in synergy with A2 partners are defined.

1.4.3 Deviation from Work plan

This deliverable represent the rewrite of D3.3.3 It has a revisit of requirements (by bringing them at a higher level of abstraction) and contains specific survey in order to allow A3 scenario to properly judge the importance of each requirement in respect to the TClouds Infrastructure built by A2 partners. At the time of writing the survey are still ongoing and have partial results, not yet valid as representative for requirement prioritization. However, the document has included the whole process: from surveys, to mapping them into the requirements, to requirements prioritization. It is intended that the actual prioritization is a preliminary result. The main reason of this delay is mainly the stakeholder's network that needs to be set-up in order to have valid interviews. More information on this can be found in chapter 3.3.1 (Survey to A3 Stakeholders, page 18) of this document.

At the end of the third year, D3.3.4 will provide a follow up of this deliverable with the results of the validation activities listed here.

1.4.4 Target Audience

Target audience of this deliverable includes all TClouds partners, especially partners from Activity 2, who wish properly evaluate and validation activities in the third year, in order to improve TClouds security solutions.

1.4.5 Relation to Other Deliverables

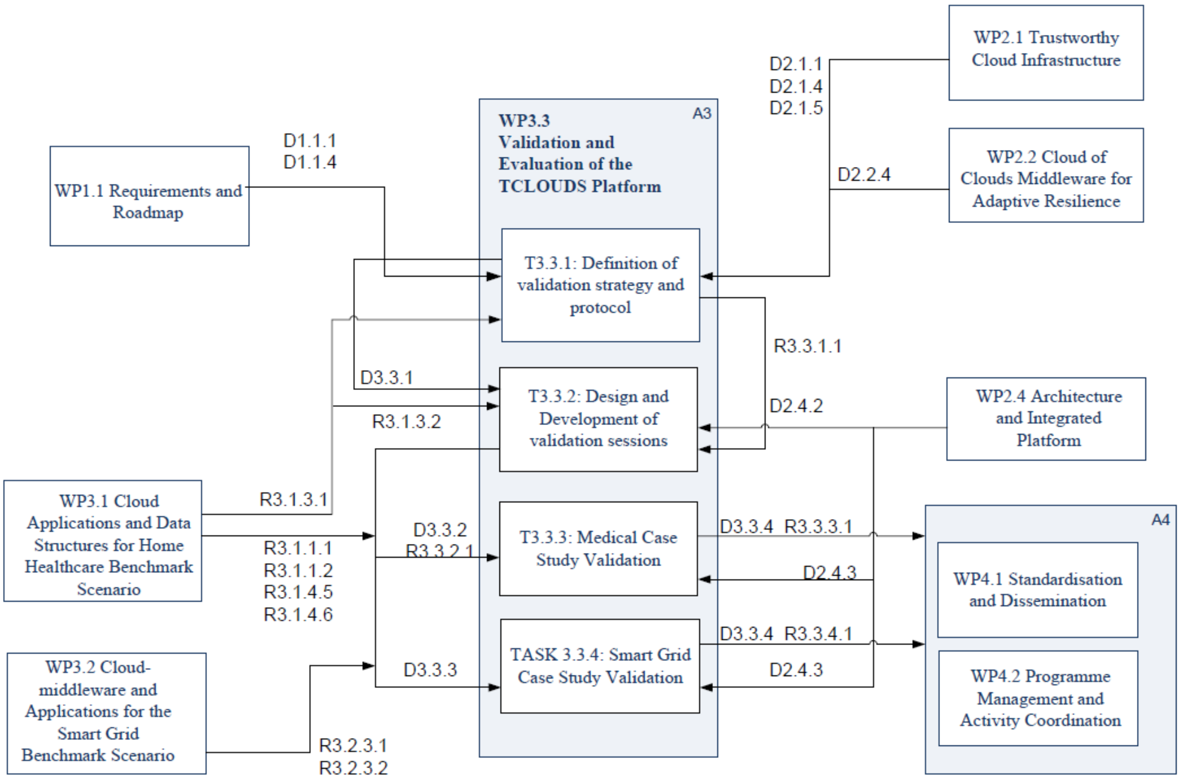
WP2.1 Trustworthy Cloud Infrastructure
D2.1.1
D2.1.4
D2.1.5
WP2.2 Cloud of Clouds Middleware for Adaptive Resilience
D2.2.4
A3
WP3.3 Validation and Evaluation of the TCLOUDS Platform
WP1.1 Requirements and Roadmap
D1.1.1
D1.1.4
T3.3.1: Definition of validation strategy and protocol
R3.3.1.1
D3.3.1
T3.3.2: Design and Development of validation sessions
R3.1.3.2
D2.4.2
WP2.4 Architecture and Integrated Platform
WP3.1 Cloud Applications and Data Structures for Home Healthcare Benchmark Scenario
R3.1.3.1
R3.1.1.1
R3.1.1.2
R3.1.4.5
R3.1.4.6
D3.3.2
R3.3.2.1
T3.3.3: Medical Case Study Validation
D3.3.4 R3.3.3.1
D2.4.3
A4
WP4.1 Standardisation and Dissemination
WP3.2 Cloud-middleware and Applications for the Smart Grid Benchmark Scenario
D3.3.3
TASK 3.3.4: Smart Grid Case Study Validation
D3.3.4 R3.3.4.1
D2.4.3
WP4.2 Programme Management and Activity Coordination
R3.2.3.1
R3.2.3.2

Figure 1 - Interdependency chart for WP3.3

This deliverable (D3.3.3 - rewrite) receives inputs from different areas of TClouds project. Specifically from WP2.4 (as you can see them reflected into the following chapters).

1.5 Changes introduced with the rewrite of D3.3.3 (V2.0)

1.5.1 Requests from reviewers

Following the main highlights about A3 and W3.3 that reviewers wrote in their Technical Review Report delivered in January 2013[1]:

Highlight 1 (page 2 of the Technical Review Report):

"Deliverable D33.3 contains a comprehensive plan for evaluating the value of various results of TClouds. In the light of the need for a clear positioning on the market of the TClouds sub-systems and use cases, the consortium is invited to focus on the sub-systems and use-cases evaluations with indicators that can be used by the marketing activities of TClouds. The weighting system used on the indicators should be validated by external stakeholders."

Highlight 2 (page 5 of the Technical Review Report):

"The validation strategy is sound. However it was expected that the weighting system for the TClouds sub-systems being defined in terms of success measures, target values, and roles. End users should be involved in the definition of the weighting system and the priorities."

Highlight 3: (page 16 of the Technical Review Report):

"The work package activities are focused on evaluation and validation of the project results, which are expected to be the ones from Al, A2 and A3 activities. A validation strategy for the two use cases and for part of the A2 sub-systems has been well defined. Concerns were raised about the aim of the procedures: while D3.3.3 is oriented towards technical measurements, a broader spectrum of measures (including performance indicators) should be taken into account to stress the sub-systems of the TClouds platform by the two applications (when these sub-systems are integrated). In the third year review it is expected to see how the two applications benefited of the TClouds platform, any lessons learned and how, thanks to which sub-system the Al requirements are met."

By considering this highlights and after an extensive discussion either during A3 meeting and EB meeting in the last internal technical meeting held in Oxford in February 2013, we concluded that the rewrite of D3.3.3 will proceed considering the following aspects:

- A2 external stakeholders will be seen as A3 partners and use cases
- A3 external stakeholders will be clearly involved via specific surveys
- A3 external stakeholders will be clearly involved via specific surveys
- It will use the same validation strategy as before since it already includes success of measures and target values and role separation
- Requirements will be rearranged and moved towards an higher-level of abstraction
- Validation Activities will be rewritten also enhancing performance/benchmarking indicators

[1] Please refer to: Technical Review Report for TClouds Project after the Review Meeting held in Brussels on November 2012

1.5.2 Approach adopted

Considering the request from reviewers, we decided to approach the D3.3.3 rewrite focusing mainly on A2 Infrastructure validation.

Following are the actions that WP3.3 will consider while rewriting D3.3.3

- A3 will weight A2's indicators since A2 stakeholders are A3's scenario.
- A3 will produce surveys specific for the two use cases with the respective use cases' stakeholders. This will allow A3 to judge and weight properly A2 indicators.
- D3.3.3 activities will be rewritten in a higher level of abstraction and they will address all the TClouds objectives. These activities will be mapped with those in D2.4.2 to address each subcomponents functionality and tailored to emphasize the requirement coverage by using the Use Case's virtual machine.
- Validation activities will be described in detail as well as their scheduling in Y3.
- D3.3.3 strategy will follow the same strategy as used before.
- Old D3.3.3 requirements will be aggregated and aligned with D2.4.2 requirements.

Chapter 2

Evaluation and Validation Strategy

Chapter Authors:

Marco Abitabile (FCSR)

2.1 General Strategy

The strategy and the protocol for the validation of the TClouds system is briefly described in the Description of Work, but it will be further detailed and conjugated here for the specific TClouds results.

First of all it's important to understand what we mean with Validation and Evaluation (which is the WP3.3 name):

PMBOK[2] says:

> *Validation: The assurance that a product, service, or system meets the needs of the customer and other identified stakeholders. It often involves acceptance and suitability with external customers. Contrast with Verification.*
>
> *Verification: The evaluation of whether or not a product, service, or system complies with a regulation, requirement, specification, or imposed condition. It is often an internal process. Contrast with Validation*

With this in mind, the goal of WP3.3 is to assess the results of the TClouds project, when possible in a quantifiable way, and otherwise in a qualitative way. Qualitative and quantitative dimensions will be gauged by the use of tools, actors and activities that best represent and describe the project's main objectives. These processes are part of the Validation phase.

The evaluation (what PMBOK call "Verification") is a second phase where results of the validation are discussed and critically analyzed. Evaluation phase will help us to identify if and where the project lacks and maintains coherence with the main TClouds objectives and will help to assess the future work that still has to be done.

The Validation process will be structured according to the following items (see Figure 2 for a graphical representation):

- **Targets of Evaluation (TOE)**: The TOE are the objects of the evaluation activity, e.g. technical features, reliability of the Cloud, security, etc.
- **Actors/perspective**: For each target of evaluation different actors can be involved, and this brings different perspectives to the evaluation results. Examples of actors may be patients, healthcare professionals, but also developers, legal or regulatory experts, etc.
- **Dimensions**: For each target of evaluation, the dimensions to be evaluated must be identified. The dimension of evaluation are the specific features the project evaluates in order to assess the achievement of the implementations of the platform.

[2] http://www.pmi.org/PMBOK-Guide-and-Standards.aspx

- **Indicators**: In order to provide the results of the evaluation for the identified evaluation targets, it is necessary to identify the indicators that express the dimensions to be investigated, i.e. provide a list of parameters to be assessed in order to respect the stated evaluation dimension of the specific target of evaluation.
- **Tools of evaluation**: The evaluation dimensions and related indicators can be investigated through different evaluation tools, for example user tests, focus groups, trial use of the system, questionnaires, interviews, comparison tests, statistics etc. Once the best instrument to assess the evaluation dimension is identified, the tool shall be designed in order to have it available for evaluation activities.
- **Criteria**: the achievement of the evaluation objective is assessed on the basis of specific criteria, i.e. the desired level of achievement for a specific indicator, for example threshold values, percentages etc.
- **Activity description**: description of the validation activity performed or planned including the involvement of the actors, the test setting, the tool proposal, the extraction of the results

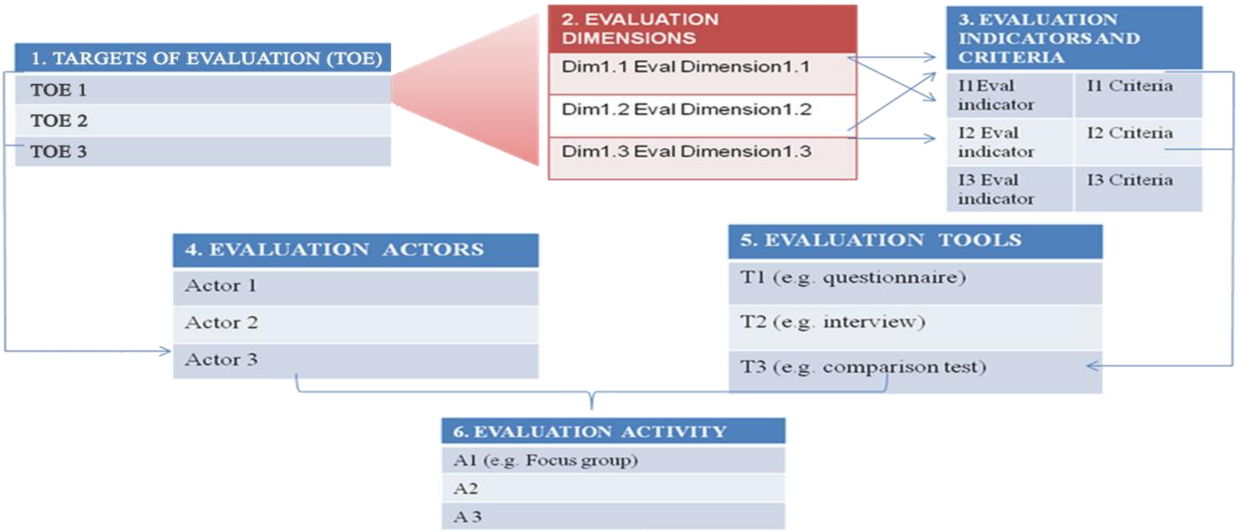

Figure 2 - General Validation Strategy

This strategy is very generic, and should be properly adapted to suit the project's needs. In TClouds project the main **TOE** identified in the validation strategy are:

1) Cloud-of-Clouds
2) Trusted Infrastructure Cloud
3) Trustworthy Openstack

Evaluation dimensions are directly represented by the requirements for each product/TOE. This document will collect them from A3 (WP3.1 and WP3.2) and the legal compartment (A1).

2.2 Validation Strategy for TClouds

Considering the general validation strategy described in the previous chapter, is now described how we will adapt it for our validation purposes.

We have divided the Validation Process in 5 main tasks:

- Requirements' list (Task1)
- Requirements' prioritization (Task2)
- Requirements' indicators definition (Task3)
- Validation Activities definition (Task4)
- Activities executions (Task5)

Tasks 1-4 are described in this document, Task 5 will be performed in period 3 and outcomes will be described in Deliverable 3.3.4 (Final Report on Validation Activities, M36).

What follows in this chapter is the methodology for Task 1-4. The outcomes can be found in Chapter 3 (Implementation of the validation strategy).

2.2.1 Requirements' list (TASK 1)

One of the first things that should be done is to make a list of all the project's requirements. This part should be easy and straightforward, since requirements' elicitation should be already done at the beginning of the project. Our approach to requirement analysis takes inspiration to the *Volere* requirement list (see: Volere Requirements Template[3]).

To make it more effective we strongly suggest to define for each requirement, the following information:

- **Requirement # and name**: a unique id of the requirement and its name
- **Description and rationale**: a one sentence statement of the intention of the requirement and its justification.

2.2.2 Requirement prioritization (TASK 2)

All the project's requirements are essential to carry out the project's tasks. Nonetheless some requirements have to be analyzed before others and have higher relevance than others. This prioritization is useful for two main reasons:

- By identifying your requirement priority you can easily understand how the development is covering this requirements (e.g.: covering many requirements but that have little importance, or cover just few requirements that have an high impact on the project)
- Understand which effort you may need in case you have to cover the requirements you have left undone.

In order to help finding the right priority, the following schema can be used:

[3] See www.volere.co.uk

Requirement #	Value/asset #1	Value/asset #2	Value/asset #3	Rating
	Value for stakeholder1	**Value for stakeholder2**	**Value for stakeholder3**	
	Factor score	Factor score	Factor score	
REQ1	2,77	2,83	2,30	2,63
REQ2	3,05	3,00	2,42	2,82
REQ3	2,48	3,33	2,53	2,78
REQ4	2,77	2,83	1,94	2,51
REQ5	2,77	3,00	1,92	2,56
REQ6	2,77	3,00	2,31	2,69
REQ7	2,49	3,00	1,92	2,47
REQ8	2,13	3,00	1,86	2,33
REQ9	2,34	2,78	1,86	2,33
REQ10	1,78	2,67	2,35	2,27
REQ11	2,49	2,81	1,93	2,41
REQ12	2,61	2,57	1,86	2,35
REQ13	3,05	3,00	1,92	2,66
REQ14	2,25	2,17	1,98	2,13

Table 1 - Prioritization example table

- **Priority rating:** sum of all weighted factors
- **Factor Score:** the score arrives from an evaluation of the given requirement for the specific stakeholder. This factor may arrive in different form: via surveys, via direct interviews, market analysis, etc.
- **Stakeholders:** define your main stakeholder, give them a weight according with your strategy and business, and place the related factor-score according to the stakeholder's importance of that specific requirements

This prioritization will be used at the end of the validation process (once the validation activities will be performed), in order to understand which requirements have been covered and their relative importance. In case some requirements are leftover we can than understand the "gravity" of the lack by evaluating their priority.

2.2.3 Indicators and Criteria (TASK 3)

Once all the relevant requirements has been finalized (Previous task, #2) we start a process that leads us to define activities that will assess and certify that the requirement has been fulfilled.

There are different approaches to do this. And we opted for a strategy to put everything in numbers: basically, it should be possible to define either qualitative or quantitative requirements with specific values (generally a percentage, relative values, Boolean values) that indicate the extent to which a requirement has been fulfilled.

Let's make few examples:

2.2.3.1 Quantitative requirement

2.2.3.1.1 Example 1

Imagine we are producing hammers, and we have a specific requirement that says that

R1: "hammers needs to have a weight of X Kg, with t% of tolerance".

In this case the indicator that can satisfy requirement R1 can be:

I1: Avg. Weight of the hammers

or

I2: % of hammers above tolerance limit

Whose criteria to satisfy the requirement can be:

x-t% < I1 < x+t%   for I1

or

I2 < 5%   for I2 (imagine that 5% is the percentage of errors we can tolerate to say that the requirement is satisfied. Vice versa, we are saying that 95% of hammers are good)

If I have to choose, I would prefer to use I2 in order to satisfy R1: it is more loosely coupled with the requirement and gives a better modeling of the real world (it explicitly extract the information of the quality of the production machinery).

2.2.3.1.2 Example 2

Sometimes requirements are difficult to translate into numbers, especially when a requirement is formulated as follows:

R2: "the perceived security from an end user has to be high"

For such a requirement you have to solve a question like: How can I quantify the 'amount' of perceived security? How can I clarify the fuzzy value "high"?

Here's an example: Make the requirement even more abstract and specify that "the perceived security is high when an end user is willing to put her data into the system". Then the Indicator can be easily found:

I2: Number of persons willing to put their data in the platform

And, accordingly, the criteria to satisfy the requirement can be:

I2 > 75%

Again, the percentage 75% may come from a business perspective. I can say that the requirement is fulfilled if at least 75% of the people involved are convinced to use the product with no security/privacy fears, hence are willing to input their data.

It's possible that some requirements are so complex that they need more than one indicator. In that case simply define each of them.

2.2.3.2 Qualitative requirement

2.2.3.2.1 Example 1

Certain requirements require a more qualitative approach to investigation. Typically, these are explorative requirements and need to be fine-tuned and taken into account in a next iteration of the test. Review the following requirement:

R3: “When a user is willing to input data in the platform, s/he should only do this when s/he perceives the security to be high.”

We can think of a number of qualitative and quantitative ways of verifying this. On the one hand, we can request the user upfront to only input data when s/he perceives the security to be high. At the end, we can simply see the percentage of people who input data. However, with this approach, we leave a large margin for error. We simply don’t know whether the people who input data did this for the right reason, and vice versa, we can’t tell that the people who didn’t input their data did so due to lack of perceived security.

In this sense we can see this requirement as being explorative, and set up a more qualitative test. We could set up a focus-group and have people look at our system, and actively discuss their perceived security. In addition, this is an excellent way of finding out which elements in your system foster the sense of security and which don’t. Results can guide us towards iterations we may not have thought of without this information.

2.2.3.3 Putting everything into table

Indicators are carried along with Activities. All the indicators will be the outcomes of the Validation activities. Once one criterion is satisfied with the execution of the corresponding activity, the given activity can be considered completed.

2.2.4 Definition of Activities (TASK 4)

Validation activities are used to assess and quantify the indicators that have been found in the previous task (Indicators and criteria).

Activities may be of different types e.g.: technical test, review, practical tests, benchmarking, stress tests. In essence the choice of activity depends heavily on your requirements and indicators. One activity can satisfy more than one Indicator and one Indicator can have several activities attached if needed.

The following template can be used to include all the necessary info for the activity.

Activity ID	Unique Id
Activity type	Proof of concept, benchmark, technical test…
Activity description	Brief description of the activity and the main steps to carry on in order to reach the criteria
Acceptance Criteria	The criteria found at the previous point
Requirements satisfied:	The list of the requirements that this activity satisfies
Reference documents:	Documents that may help in executing the activity

Table 2 - Activity template

Chapter 3

Implementation of the validation strategy

Chapter Authors:

Marco Abitabile (FCSR)

Nuno Emanuel Pereira, Miguel Areias (EDP)

Paulo Jorge Santos (EFACEC-ENG)

Kees Wouters, Yvon Peters (PHI)

3.1 Identification of Stakeholders

In this chapter is described the identification and the description of the main A3 stakeholders. The list is written considering the last version of Home Healthcare and Smart Lighting System scenario. With the sentence “main A3 stakeholders” we refer to all those stakeholders that are the final hands-on users of the two A3 applications and have certain expectancies in terms of privacy, security and availability of the data managed.

3.1.1 A3 stakeholders

3.1.1.1 Identify stakeholders

3.1.1.1.1 Home Healthcare

In regards with the Home Healthcare platform described in D3.1.3[4] we can identify 3 main stakeholders of the platform:

- **Developer**. This is a (possibly external) party that produces applications related with health. These applications connect to the platform to interact with health data of the users.

  Profile description: they are mainly interested in security and privacy of data and in availability of the system. They have high IT competencies and might be employees of big SW companies that produce professional health applications (such as applications for hospitals or health devices) as well as entrepreneurs and hobbyist people that like to program and develop health-related apps.

- **Patient.** She/he can be considered as the main stakeholder. Thanks to this actor the platform has a reason to exist since all the data is Patients’ data. With this actor we can identify ill people, people with chronic diseases, but also health-savvy people and anyone that may generate any kind of health data (from EHR[5] type to PHR[6] type)

[4] See: http://www.tclouds-project.eu/downloads/deliverables/TC-D3.1.3_Draft_proof_of_concept_for_home_healthcare_M24.pdf

[5] EHR: this type of data are data generated from professional people, generally doctors or medical certified devices in regards of patient’s health

Profile description: Patient stakeholders are a very diverse type of people. At this stage of the development we are not going to dig more into this type of users. The main subcategories that can be identified are:

- Very old / very young people that are “passive” with respect of the platform usage. Their data flows into the platform because someone else is placing them (such as a doctor or a dear close person)
- Adult active people: their age spans from 15-18 up to 50-60 year old, they are actively contributing in health data collection either via devices or application. They mainly produce PHR data that can arrive through their doctors. They are inclined to use high-tech devices and are familiar enough with technology.
- Adult passive people: their age spans from 15-18 up to 50-60. They do not contribute in generating health data and their data comes to the platform mainly as EHR data generated by doctors.

- **Doctors**: into this category many types of health professional can be found. We now focus mainly to doctors working in hospitals, such as doctors of San Raffaele Hospital. They are professionals specialized in specific health sectors. Most of them are not inclined to use the technology and they have really little time available. Age spans from 28-30 up to 60+ years old.

There are many others stakeholders, such as pharmacies, researchers, app managers, independent doctors (such as GP), doctors working in an hospital/big institution, insurance companies, employers, employees, personal trainers… but for the actual interest of the TClouds infrastructure development we decided to focus on these three types.

3.1.1.1.2 Smart Lighting System

Regarding the Smart Lighting System described in D3.2.3[7], we identified three main Smart Lighting System stakeholders which can be characterized as follows:

- **Municipalities:** In Portugal, a municipality is an administrative division of the country with administrative autonomy over certain public matters, including public lighting management. Portuguese municipalities are responsible for deciding the public lighting schedule; by other words, they decide when public lighting should switch on or off.
- **Utilities:** In Portugal, the utility is responsible for public lighting control execution according to the schedules defined by municipalities. This role is occupied by different stakeholders in some other countries.
- **Vendors:** These are the suppliers of the public lighting management system.

[6] PHR: this is a broad type of data. It consists of any type of data that can be, directly or indirectly, related to a person health. PHR data can vary, from environmental temperature to pollution of the air to weight measurements, to physical activity, to food eaten, to blood pressure and so on.

[7] See: http://www.tclouds-project.eu/downloads/deliverables/TC-D3.2.3_Smart_Lighting_Draft_Prototype_M24.pdf

3.1.2 A2 stakeholders

3.1.2.1 Identify stakeholders

Identification of A2 stakeholder has been straight-forward. As stated in chapter 1.5 – Approach Adopted – we identified the external stakeholders of A2 as the two benchmark scenario of TClouds. That is, the Smart Lighting System and the Home Healthcare scenario.

3.2 Identification of Requirements for A2 based on A3 needs (TASK 1)

Recalling Chapter 4.1 (Mapping on prototype subsystems and old D3.3.3 requirements) and chapters 2.1 and 2.2 of D2.4.2, here the list of A2 requirements against A3 and legal framework

3.2.1 Legal requirements

These high level objectives have to be interpreted and applied to specific technical infrastructures like cloud computing. They need to be addressed at four different levels: organizationally, contractually, technically on application level and technically on infrastructure level. Only in combination those four levels of security measures can provide adequate comprehensive solutions.

The opportunities and interplay of these layers of measures will be further described and analyzed in D1.2.3 and D1.2.4. The security objectives that can be derived from European legislation need to counter the specific risks that cloud computing poses regarding data protection and privacy. These risks will be identified in detail in D1.2.4 Cloud Computing – Privacy Risk Assessment. Without prejudice to national laws, there are key areas of privacy risks and the corresponding security objectives. The TClouds subsystems for a trustworthy internet-scale computing platform address these legal security objectives mainly on infrastructure level and a few on application level, so the following requirements focus only on technical security measures. Please note that for meeting the identified security objectives there may exist several suitable measures. Often some of these have to be combined to achieve the best result.

Defined legal requirements are:

LREQ1 - Confidentiality of personal data: The Cloud Provider must prevent the breach of users' personal data by securing the infrastructure (including the internal network) and ensuring the isolation among different tenants. Further, he must avoid accesses on data by unauthorized entities through accesses management or, at least, must record relevant events through an auditable logging mechanism (that also logs actions performed by Cloud provider's employees). Confidentiality can be achieved also by encrypting data in a way that decryption would be possible only for customers.

LREQ2 - Availability and Integrity of personal data: The Cloud Provider must prevent the loss or manipulation of users' personal data through Duplication and Distribution (this poses some new risks, please refer to D1.2.3).

LREQ3 - Control of location (country wise) and responsible provider (cloud subcontractor): The Cloud Provider must guarantee the applicability of law for processing personal data through location audit trails for the customer and safeguards that prevent data transfer to Cloud premises in other locations than those explicitly agreed with the customer.

LREQ4 - Unlinkability and Intervenability: The Cloud Provider must prevent unauthorized pooling, combining and merging of data through anonymization, pseudonymisation and splitting of data, through encryption of personal data (decryption only by customer) or isolation of tenants. The Cloud Provider must prevent the loss of control of data due to unauthorized copies through the encryption of data (with decryption by customers) or the effective and complete deletion. He must also provide to customers extensive control functions to avoid the risk of hindrance of the data subject's rights of access, rectification, erasure or blocking of data.

LREQ5 - Transparency for the customer: The Cloud Provider must inform his customers about the security measures adopted to protect their personal data against loss of control due to unauthorized copies, manipulation, unauthorized pooling, combining and merging. The Cloud Provider must also prove that he did not circumvent the security measures chosen by providing customers with an auditable logging of accesses made by himself and his employees.

3.2.2 Healthcare requirements:

The TClouds healthcare application scenario focuses on developing a cloud-supported healthcare application to provide collaborated services across different health care providers.
The choice of adopting the technologies introduced by Cloud Computing was led especially by the significant costs required to provide a service accessible by remote users. These costs arise either for building and maintaining a dedicated IT infrastructure within the hospital or for outsourcing this service to an external organization that requires periodic payments regardless of the resources usage.

Cloud computing provides a solution to the above problem as it combines the outsourcing model with a pay-per-use model, enabling low entrance barriers and substantial cost reductions when no services are received or less resources are used. In addition, cloud computing offers scalability, because it allows to transparently add more resources to the service if there is an increase in demand, availability and resilience because a typical Cloud infrastructure is built to support a large number of customers and, finally, increased connectivity through redundant Internet connections.

However, hosting a service in a Cloud introduces security risks that do not apply to a dedicated IT infrastructure. The main objection to the adoption of Cloud Computing (65%) in the BridgeHead survey was the hospitals' concerns about the security and availability of healthcare data given the great number of threats, including privacy breaches and identity theft. Other objections include cost (26.1%) and a lack of confidence that Cloud offers greater benefits with respect to local storage media (26.1%). Current Cloud systems suffer from drawbacks and do not offer the expected Cloud infrastructure characteristics.

In the following, we present the revised security and privacy requirements that must be satisfied by the infrastructure to run the healthcare application in the Cloud environment.

AHSECREQ1 - Confidentiality of stored and transmitted data:
Prevent that an attacker can retrieve and disclose data from the patient data repository or information transmitted through the communication channel between the personal front end and the management application.

AHSECREQ2 - Integrity of stored and transmitted data:
Detect corruption done by an attacker of data stored in the patient data repository or exchanged through the communication channel between the personal front end and the management application.

AHSECREQ3 - Integrity of the application:
Detect corruption of the management application done by an attacker to modify its functionality.

AHSECREQ4 - Availability of stored and transmitted data:
Prevent Denial-of-Service attacks to the patient data repository or to the communication channel between the personal front end and the management application.

AHSECREQ5 - Availability of the application:
Prevent Denial-of-Service attacks to the management application.

AHSECREQ6 - Non repudiation:
Prevent that an attacker denies the fact that he/she has ever performed a specific action (e.g. he/she made the data available to unauthorized parties).

AHSECREQ7 - Accountability:
Detect actions done by an attacker to provide him/her with privileges for the patient that should not be assigned to him/her.

AHSECREQ8 - Data source authentication:
The attacker must not be able to run a process that appears as the legitimate management application.

AHPRIVREQ1 - Unlinkability and Anonymization of data flow:
Use data anonymization/pseudonymization techniques to anonymize/pseudonymize the documents stored in the data store and enforce process confidentiality (e.g. the state, the memory and administrative interfaces of the process) by means of strong/secure access control.

3.2.3 Smart Lighting System Requirement

The purpose of the TClouds Energy application scenario is to develop a Public Light Management solution available online for Municipalities and the Utility operators. Traditionally, this type of solution would be hosted in the Utility Datacenter, mostly due to the required elements be already in place (D3.2.3 [SV12], Chapter 3).

Within TClouds, this solution is to be hosted initially in a commodity cloud environment, and then integrated with TClouds security components. In this way, we will investigate not only the constraints and feasibility of the migration to a cloud environment, but also the cost-benefits for adopting TClouds.

The following security requirements were specifically collected from “D3.3.3 – Validation Protocol and Schedule for the Smart Lighting and Home Health Use Cases” ([AN12]), within the Energy use case context.

ASSECREQ1 - Trustworthy Audit: Smart Lighting actions (application access, create, update, and delete data) must be fully audited, and accessible only to privileged users.

ASSECREQ2 - Trustworthy Infrastructure: The hosting infrastructure must prevent intrusions.

ASSECREQ3 - Trustworthy Persistence Engine: The persistence engine must prevent intrusions and ensure confidentiality, integrity and availability.

ASSECREQ4 - Resilient: The Smart Lighting System must be fault-tolerant at infrastructure and at persistence level.

ASSECREQ5 - Trustworthy communications: Communications between a client and the Smart Lighting System must prevent data from being altered by using adequate security mechanisms.

ASSECREQ6 - High performance & Scalable: The Smart Lighting System must have near real-time performance, and be able to scale on increased load.

3.2.4 Requirements coverage

The diagram below describes, in a glance, the coverage of the requirements by the TClouds Infrastructure

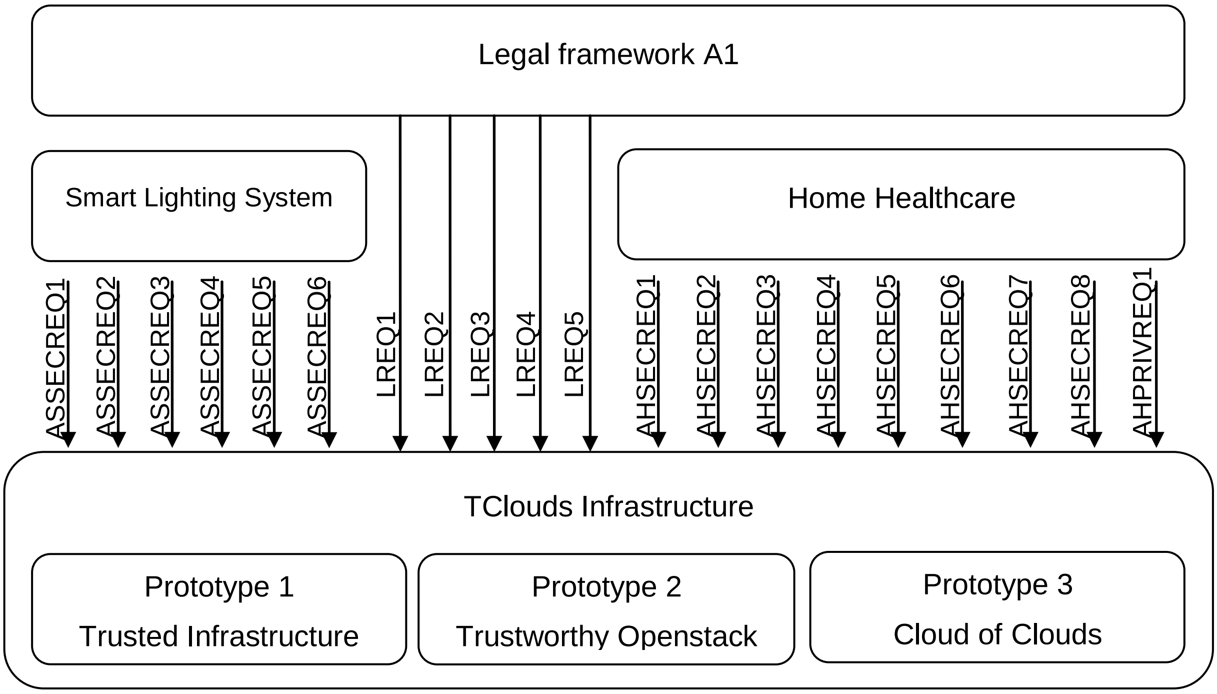

Figure 3 - Requirements coverage by TClouds Infrastructure

3.2.5 Mapping on prototype subsystems and old D3.3.3 requirements

In order to maintain continuity with the effort spent in the old D3.3.3 document in appendix (4.1 - Mapping on prototype subsystems and old D3.3.3 requirements) is described the mapping between old Requirements and new ones. This mapping is useful also during the validation activity phase, in which some activities are derived from the old D3.3.3 and can be easier mapped to the specific requirement satisfied.

3.2.5.1 What is not included in this document

Some components of the TClouds Infrastructure are not directly used by the two use cases.

While building the two A3 benchmark scenario, we strived to embrace and use all the features that TClouds Infrastructure can provide us. However, not all of them have been directly used by A3. These unused components are:

- Confidentiality proxy for S3
- Fault-tolerant Workflow Execution (FT-BPEL)
- Automated Validation (SAVE)

Considering that this document has the scope of validation of the subcomponent used by the two benchmark scenarios, the three subcomponents in the list above will not be included into this document. However, they will be considered while performing the final validation results and outcome will be delivered in D3.3.4 as part of the TClouds project and addressing specific TClouds Objective.

More concretely:

- Confidentiality for S3 is an independent component that can be used at PaaS and SaaS level directly. It uses internally the same features of BFT-SMART, already included by A3 use cases, and does not add extra layer of security in the scope of A3 use case.

- Fault-tolerant Workflow Execution (FT-BPEL) is, as the previous component, an high level functionality that can be used either at PaaS and SaaS level. It uses a language (BPEL) that requires a high decoupling of the different logical functionalities within an application. Either the Home Healthcare and The Smart Lighting System uses programming techniques that makes it difficult and effort consuming to produce a porting of the appliances in order to use BPEL. However FT-BPEL used in conjunction to the TClouds Infrastructure provide an extra layer of security, especially for the delicate business procedures that occur within an application such as Home Healthcare and Smart Lighting System. In D3.3.4 this components will be tested and proved using a valid storyline taken from one of the two scenarios.
- Automated Validation (SAVE) is a component that is used mostly at cloud admin level and will be evaluated separately and independently as an extra feature that cloud provider have to ensure security.

3.3 Prioritization of requirements (TASK 2)

3.3.1 Survey to A3 Stakeholders

The surveys that A3 will do, focus on three main TClouds aspects: security, privacy and availability of the data. The overall idea is to produce meaningful values that are useful to evaluate the importance of these three aspects for the stakeholders as defined in chapter 3.1 - Identification of Stakeholders. This is translated into a precise score that represents the importance of a given requirement for a specific stakeholder.

3.3.1.1 How to interpret the survey results

At the time of writing, as stated in chapter 1.4 – deviation from work plan – the outcome of the surveys is not yet complete since the surveys are still in progress. During M30 and M31 PHI, FCSR and EDP wrote and set-up the surveys and organized the network of stakeholders to be contacted. In M30, once the surveys have been completed, A3 started to ask the stakeholders to fill in the questionnaires. However, dealing especially with doctors and municipalities has his downside: very often these stakeholders are not technology oriented and it is necessary to personally interview them to explain the meaning of TClouds and of our case studies in particular. All this results in it taking more time than anticipated.

Nonetheless, in this chapter are described the surveys in their details and the process that brings the survey’s results down into the final requirement weight.

In D3.3.4 final weights coming from surveys presented in this document, in conjunction with validation activities results, will be used to actually score the final TClouds Validation Process.

3.3.1.2 Healthcare Survey

The survey for the Healthcare scenario is composed of 3 questionnaires. They are tailored according to the three main stakeholders: Developers, Doctors and Patients.

The main focus of the three surveys is the sensitivity of the interviewees with respect to Security, Privacy and Availability of the health data.

Moreover, some questions have been introduced to provide more hints at business requirements. The results of these questionnaires will be evaluated and used in D1.3.3 due in M36.

3.3.1.2.1 Strategy adopted

In order to rank all 15 requirements, the requirements were divided in three groups, on basis of the subject they discuss (Security, Privacy and Availability).The topics were chosen from an end-user point of view, All the surveys start with the question to rank the three main topics, which defines the importance of these topics for the respondents.

The functional requirements were (partly) reformulated or supplemented by examples, to make them understandable for the target groups. In the surveys, we call the reformulated requirements “sentences”.

In the following questions, respondents had to rank 4 to 7 sentences that discuss one of the main topics, on basis of importance to them. This gives a better understanding of the requirement’s priority per topic.

The ranking approach was chosen (instead of, for example, rating) to avoid the ceiling effect, which occurs when respondents tend to place their answers close to the extreme values. This behavior was expected due to the sensitive aspects of the questions that revolve around the concept of Security, Privacy and Availability of data.

Scoring Calculation:

The following example explains the calculations applied to score the sentences in order to properly weight the requirements:

Question1: //the question used to bias the following ones.

Rank these topics, from the most important to the least important:

- Transparency & trust
- Availability
- Security

Question2: //question related to Transparency and Trust

Question3: //question related to Availability

Question4: //question related to Security

Example:

An example of scored sentences:

Q1:

- Transparency & Trust (category score = 10)
- Availability (category score = 8)
- Security (category score = 9)

Highest score in the category is always 10, lowest score in the category is always 1 Everything in between is divided over the scale.

Q2 about Transparency & Trust:

  - 1st = 10 points
  - 2nd = (9/5)*4+1+1= 8.2 points
  - 3rd = (9/5)*3+1= 6.4 points
  - 4th =(9/5)*2+1= 4.6 point
  - 5th = 1 point

- Example Sentence1 (Importance = 4th → Score = 1.0 * 4.6 = 46)
- Example Sentence2 (Importance = 5th → Score = 1.0 * 1 = 10)
- Example Sentence3 (Importance = 1st → Score = 1.0 * 10 = 100)
- Example Sentence4 (Importance = 3rd → Score = 1.0 * 6.4 = 64)
- Example Sentence5 (Importance = 2nd → Score = 1.0 * 8.2 = 83)

Q3 about Availability:

  - 1st = 10 points
  - 2nd = (9/2)*1+1= 5.5 points
  - 3rd = 1 point

- Example Sentence1 (Importance = 9 → Score = 0.8 * 5.5 = 4.4)
- Example Sentence2 (Importance = 8 → Score = 0.8 * 1 =.0.8)
- Example Sentence3 (Importance = 10 → Score = 0.8 * 10 = 8)

Etcetera…

3.3.1.2.2 Questions

Please, refer to the appendix (Chapter 4 – Healthcare Service) to see all the questions for the three healthcare stakeholders.

3.3.1.2.3 Outcome

Since the surveys are still ongoing, results will be presented in D3.3.4. In D3.3.4 requirements will be prioritized as described in Ch. 3.3 - Prioritization of requirements (TASK 2). Once requirements will be prioritized they will be used in conjunction with the outcome of the validation activities in order to evaluate TClouds project in respect to Healthcare and Smart Lighting System use cases.

3.3.1.3 Smart Grid survey

3.3.1.3.1 Strategy adopted

With reference to Ch. 4.2 (Smart Lighting System Survey): for requirements 1 to 5 (questions 1 to 5), the final score of each requirement will be achieved by calculating the average value of the answers that are given to corresponding questions (see mapping table Table 4, page 22). The final score of requirement 6 will be obtained in two steps. First, the averages of questions 6 and 7 will be calculated. Then the average of the two will be the final score.

Questions 8, 9 and 10 will not contribute to the requirements table. Instead, by comparing some requirements directly, they will support validation of results obtained.

3.3.1.3.2 Questions

Please refer to the appendix (4.2 – Smart Lighting System Survey) to see all the questions for the three Smart Lighting System stakeholders.

3.3.2 Mapping Questionnaire with requirements

The questionnaire performed for the two use cases needs to be mapped to A3 requirements for A2 prototypes in order to correctly weight and prioritize them.

Requirement #			LREQ1	LREQ2	LREQ3	LREQ4	LREQ5	AHSECREQ1	AHSECREQ2	AHSECREQ3	AHSECREQ4	AHSECREQ5	AHSECREQ6	AHSECREQ7	AHSECREQ8	AHPRIVREQ1
Survey for Developer	Q2	S1					x		x				x		x	
		S2					x		x	x			x	x	x	x
		S3														x
		S4														x
		S5						x								x
	Q3	S1									x	x				
		S2									x	x				
		S3		x												
	Q5	S1				x								x		
		S2	x					x								
		S3	x													
		S4			x											
Survey for Patients	Q2	S1												x		
		S2												x		
		S3					x		x				X	x		
		S4					x		x				X	x		
		S5					x		x				x	x		x
		S6														x
	Q3	S1									x					
		S2									x					
		S3									x					
		S4										x				
		S5														
		S6														
		S7														
	Q4	S1			x											
		S2		x											x	
		S3	x			x		x								
		S4					x									
		S5					x			x						x

Requirement #			LREQ1	LREQ2	LREQ3	LREQ4	LREQ5	AHSECREQ1	AHSECREQ2	AHSECREQ3	AHSECREQ4	AHSECREQ5	AHSECREQ6	AHSECREQ7	AHSECREQ8	AHPRIVREQ1
	Q5	S1														
		S2														
		S3														
		S4														x
		S5														x
		S6														x
Survey for Doctor	Q2	S1														
		S2					x					x	X	x		
		S3					x					X	x	x		
		S4										x		x		
	Q3	S1														
		S2									x	x				
		S3														
		S4														
		S5									x	x				
		S6									x	x				
		S7														
	Q4	S1			x											
		S2	x	x		x	x	x		X						
		S3	x			X										
		S4														
		S5														x

Table 3 - Mapping between Healthcare Surveys questions and Requirements

Requirement #		ASSECREQ1	ASSECREQ 2	ASSECREQ 3	ASSECREQ 4	ASSECREQ 5	ASSECREQ 6
Q1		x					
Q2			x				
Q3				x			
Q4					x		
Q5						x	
Q6							x
Q7							x
Q8	S1		x	x			
	S2				x		
Q9	S1	x				x	
	S2						x
Q10	Yes			x			
	No				x		

Table 4 - Mapping between Smart Lighting System survey's questions and Requirements

Each “x” in the tables above corresponds to a specific score derived from the survey results. The final weight for each requirement will be the mean of all the scores for the given requirement.

3.4 Criteria, Activities definition and scheduling (TASK 3, 4)

The Smart Lighting System and the Home Healthcare scenario are designed to work on a specific subset of features available from the TClouds Infrastructure.

Referencing to the three prototypes composing the TClouds Infrastructure presented in M24, here is depicted which features will be used by each scenario to satisfy their specific requirements

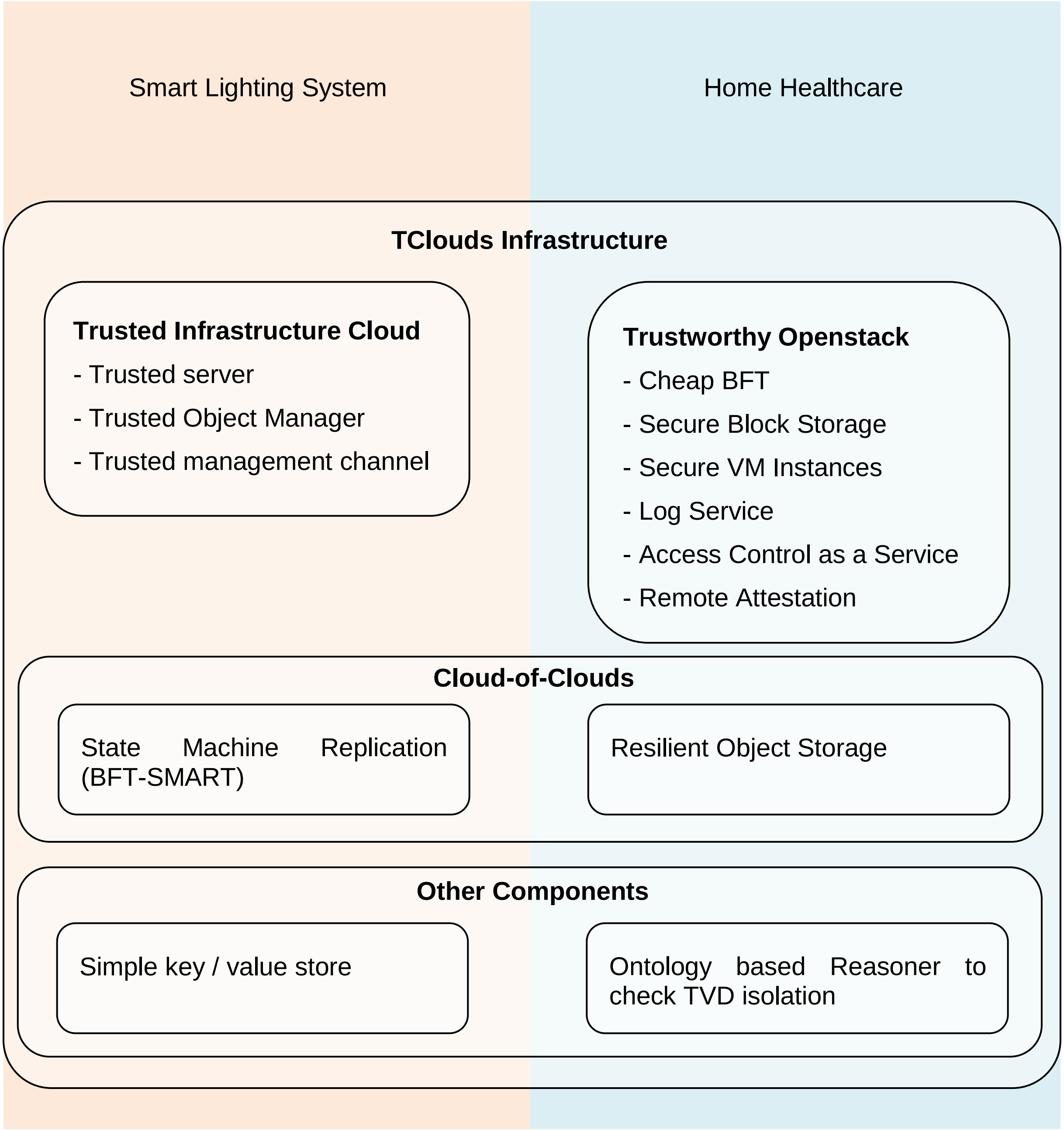

Figure 4 - Diagram describing which TClouds components are used by the two A3 scenario

3.4.1 Organization of activities

Validation activities will be performed by FCSR and EDP during M33. The two use cases will work in synergy with A2 partners in order to perform every validation activity and assess their outcome.

The following table summarizes all the activities and the requirements they assess. A requirement is reached only when all tests are successfully passed, thus compliance is reached.

requirement	LREQ1	LREQ2	LREQ3	LREQ4	LREQ5	AHSECREQ1	AHSECREQ2	AHSECREQ3	AHSECREQ4	AHSECREQ5	AHSECREQ6	AHSECREQ7	AHSECREQ8	ASSECREQ1	ASSECREQ2	ASSECREQ3	ASSECREQ4	ASSECREQ5	ASSECREQ6
Validation activity																			
SBS + SVM 1	x	x				x	x												
LogService 1	x		x	x	x						x	x		x					
CheapBFT 1		x					x	x	x	x			x						
CheapBFT 2		x					x	x	x	x			x						
DepSky 1	x	x				x	x												
DepSky 2	x	x				x	x												
ACaaS 1			x																
Remote 1					x						x	x							
Integration 1															x				
Integration 2															x				
Integration 3															x				
Integration 4																	x		
Integration 5																		x	
Integration 6																			x
Integration 7																			x
Trusted O 1															x				
Trusted O 2															x				
Trusted O 3															x	x			
Trusted S 1	x														x				
Trusted S 2	x														x				
Trusted S 3	x															x			
Trusted C 1	x		x															x	
Trusted C 2	x		x															x	
BFT-Smart 1		x														x	x		
BFT-Smart 2		x														x	x		
BFT-Smart 3		x														x	x	x	
BFT-Smart 4		x														x	x		
BFT-Smart 5		x														x	x	x	

Table 1 - mapping between requirement and validation activities

NOTE:
From the table above and from Figure4 it might be noticed that ASSECREQ1 is satisfied by the LogService component that is not used by the Smart Lighting System. It has been decided to not use the LogService component into SLS since it is used in the Healthcare scenario and already validated by activity "LogService1".

3.4.2 Description of activities and related success criteria

In this chapter and subchapters is described each single activity, the component involved and the success criteria to satisfy the activity.

3.4.2.1 Home Healthcare Activities description

3.4.2.1.1 Secure Block Storage + Secure VM Instances

Activity ID	**SBS+SVM_1**
Activity type	Proof of concept
Activity description	The Home Healthcare appliance is deployed and running onto the Trustworthy Openstack TClouds prototype. The Home Healthcare databases VMs are encrypted according to the description in the reference documents 1- Import the certified key and encrypt the Home Healthcare VMs images 2- Upload the encrypted images into the Trustworthy Openstack TClouds prototype 3- Launch the Virtual Machines 4- Cloud administrator continuously tries to hexdump on the Home Healthcare VMs 5- Cloud administrator continuously tries to make hipercalls to do introspection
Acceptance Criteria	The activity is passed if either point 4 and 5 continuously fails after 10 attempts
References Documents:	(TClouds factsheet 03 - Cryptography) (Deliverable D2.1.2, 2012) (Deliverable D2.4.2, 2012)

3.4.2.1.2 Log Service

Activity ID	**LogService_1**
Activity type	Proof of concept test
Activity description	The Home Healthcare appliance is deployed and running onto the Trustworthy Openstack TClouds prototype. The Log service is up and running as well. The Home Healthcare appliance will perform activities in order to stress the Log Service and proof its capabilities 1- From the auditing feature of the Home Healthcare appliance make a request to retrieve the logging session 2- Perform a request of verification of the logging session 3- Perform a download of the verified log as dump 4- Request and analysis of logs via the Remote Attestation Service 5- Compromise the log storage by simulating an intrusion at application level 6- Request another verification of the logging session 7- Compare the results
Acceptance Criteria	At point 7, after the verification, the system should warn the user that someone tried to compromise the log and a malicious action has been involved. Outcome: TRUE if verification fails. FALSE otherwise
Reference documents:	(TClouds factsheet - Log as a Service, 2013) (Deliverable D2.4.2, 2012) (Logging handlers) (Deliverable D2.1.2, 2012)

3.4.2.1.3 Resource Efficient BFT (CHEAP-BFT)

Activity ID	**CheapBFT_1**
Activity type	Proof of concept
Activity description	The Home Healthcare appliance is deployed and running onto the Trustworthy Openstack TClouds prototype. The Home Healthcare databases VMs are mirrored according to the Cheap-BFT component capabilities as described in references documents 6- Initiate the databases virtual machines and all the needed replicas 7- Request the health data of a specific user into the system by using either the Home Healthcare platform web interface or a third party application using the REST-API of the platform 8- Compromise one of the replicas by changing health data of

	that specific patient 9- Perform the same request as in step 2 10- Compromise, again, another replica (by bringing the compromised replicas to 2) 11- Perform the same request as in step 2
Acceptance Criteria	The activity must return the same data of step 2 in step 4. On step 6 the data retrieved is either a compromised replica or the Home Healthcare appliance thrown an error message of invalid data.
References Documents:	(TClouds factsheet 09 Cheap BFT, 2013) (Deliverable D2.1.2, 2012) (Resource Efficient Byzantine Fault Tolerance, 2012) (Deliverable D2.4.2, 2012)

Activity ID	**CheapBFT_2**
Activity type	Stress test
Activity description	The Home Healthcare appliance is deployed and running onto the Trustworthy Openstack TClouds prototype. The Home Healthcare databases VMs are mirrored according to the Cheap-BFT component capabilities as described in references documents 1- Initiate the databases virtual machines and all the needed replicas 2- Continuously request the health data of a specific user into the system by using a third party application using the REST-API of the platform 3- Continuously Compromise one of the replicas by changing health data of that specific patient
Acceptance Criteria	The Activity is passed if the outcome at step 2 is always the same for 6 hours of running the test.
References Documents:	(TClouds factsheet 09 Cheap BFT, 2013) (Deliverable D2.1.2, 2012) (Resource Efficient Byzantine Fault Tolerance, 2012) (Deliverable D2.4.2, 2012)

3.4.2.1.4 Resilient Object Storage (DepSky)

Activity ID	**DepSky_1**
Activity type	Proof of Concept
Activity description	The Home Healthcare appliance is deployed and running onto the Trustworthy Openstack TClouds prototype. The PHR database VM has installed the DepSky drivers 1- From the Home Healthcare administrator interface define all the setup information to connect to the different cloud providers 2- Define a file span of 2MB per file 3- Perform a snapshot of the PHR databases by zipping and spanning the file 4- Send the files on the different cloud by using the DepSky driver 5- Check in the commodity clouds that the file is saved correctly 6- Take a file from the commodity cloud account and check the encryption 7- Remove a file from one commodity cloud 8- From the healthcare administrator console perform a restore of an old backup 9- Check that the backup data is consistent as the original backup 10- Confirm that only by having f+1 shares of the secret is possible to decrypt data
Acceptance Criteria	The Activity is passed if: • At point 5 all the files results correctly saved • At point 6 all the data are encrypted • At point 9 the restored data is the same as the original backup • Point 10 has to be confirmed
References Documents:	(Deliverable 2.2.1, 2010) (Deliverable D2.4.2, 2012) (Depsky, 2011) (C2FS)

Activity ID	**DepSky_2**
Activity type	Benchmarking
Activity description	The Home Healthcare appliance is deployed and running onto the Trustworthy Openstack TClouds prototype. The PHR database VM has installed the DepSky drivers 1- From the Home Healthcare administrator interface define all the

	setup information to connect to the different cloud providers 2- Define an incremental file span from 1MB up to 10 MB per file 3- Perform a snapshot of the PHR databases by zipping and spanning the file 4- Send the files on the different cloud by using the DepSky driver 5- From the healthcare administrator console perform a restore of an old backup 6- Calc the time requiring to restore the backup for each file dimension
Acceptance Criteria	The Activity will be judged by benchmarking the latency of read/write operation compared by using a single commodity cloud
References Documents:	(Deliverable 2.2.1, 2010) (Deliverable D2.4.2, 2012) (Depsky, 2011) (C2FS)

3.4.2.1.5 Access Control as a Service (ACaaS)

Activity ID	**ACaaS_1**
Activity type	Proof of Concept
Activity description	The Home Healthcare appliance is deployed and running onto the Trustworthy Openstack TClouds prototype. The Home Healthcare platform is composed of 4 VMs: 1 Appliance VM, 2 EHR Database VMs, 1 PHR Database VM. While the latter one has no restriction on location or exclusion, the Appliance and EHR databases needs specific restrictions. 1- Deploy a Fake VM representing an appliance of a Bank Institution 2- Deploy the Appliance VM with the following requirements: a. The VM should not run in the same physical machine of a Bank Institution b. The VM should not run in the same physical machine of the EHR Database VMs 3- Deploy one EHR VM with the following requirements a. The VM should not run in the same physical machine of a Bank Institution b. The VM should not run in the same physical machine of the other EHR Database VM and of the Appliance VM c. The VM should run on physical machines located in Italy 4- Deploy the other EHR VM with the following requirements a. The VM should not run in the same physical machine of a Bank Institution b. The VM should not run in the same physical machine of the

	first EHR Database VM and of the Appliance VM c. The VM should run on physical machines located in Germany 5- Check whether the requirements has been respected by manually inspecting the VM deployment 6- Try to migrate each VM into hardware that does not respect the requirements
Acceptance Criteria	The Activity is passed if: • At Point 5 all the VMs are deployed correctly • At point 6 no VM could be migrated
References Documents:	(Deliverable D2.3.2) (Deliverable D2.4.2, 2012)

3.4.2.1.6 Remote Attestation

Activity ID	**Remote_1**
Activity type	Proof of Concept
Activity description	The activity can be performed in conjunction of activity ACaaS_1. The Remote attestation checks are executed right after point 5 and 6
Acceptance Criteria	The Activity is passed if: • The remote attestation attests the same results of the manual check at point 5 and 6 of activity ACaaS_1
References Documents:	(Deliverable D2.4.2, 2012) (Intel Open Attestation SDK)

3.4.2.2 Smart Lighting System Activities description

3.4.2.2.1 Integrated TClouds SLS system

Activity ID	**Integration_1**
Activity type	Benchmarking
Activity description	Evaluate the infrastructure trustworthiness to prevent intrusions. 1- Confirm access to SL hosts employs state of the art secure mechanisms (ex. secure protocols; certificates)
Acceptance Criteria	Step 1 is successful

Activity ID	Integration_2
Activity type	Benchmarking
Activity description	Evaluate the *persistence engine* trustworthiness to prevent intrusions. 1- Confirm access to the *persistence engine* employs state of the art secure mechanisms (ex. secure protocols; certificates)
Acceptance Criteria	Step 1 is successful

Activity ID	Integration_3
Activity type	Benchmarking
Activity description	Evaluate the *persistence engine* confidentiality. 1- Confirm data stored within the *persistence engine*, is only readable by authorized sessions.
Acceptance Criteria	Step 1 is successful

Activity ID	Integration_4
Activity type	Stress Test
Activity description	Evaluate the *persistence engine* resiliency ratio, when the number of faults is within the designed tolerance. 1- Being *f* (tolerated faults) nodes unreachable and 2 SL App nodes, with an automated script execute through SL Business Layer interface, 10, 20 and 100 simultaneous sessions doing: • 100 create actions over: Schedules; Users • 100 edit actions over: Schedules; Users • 100 delete actions over: Schedules; Users • 10 successful logins & logouts • 10 unsuccessful logins 2- Being *f* nodes compromised (reachable but with un-synched data) and 2 SL App nodes, with an automated script execute through SL Business Layer interface, 10, 20 and 100 simultaneous sessions doing: • 100 create actions over: Schedules; Users • 100 edit actions over: Schedules; Users • 100 delete actions over: Schedules; Users • 10 successful logins & logouts • 10 unsuccessful logins 3- Being all nodes online and 2 SL App nodes, with an automated script execute through SL Business Layer interface, 10, 20 and

	100 simultaneous sessions doing (while doing it, cut the cord to *f* nodes): • 100 create actions over: Schedules; Users • 100 edit actions over: Schedules; Users • 100 delete actions over: Schedules; Users • 10 successful logins & logouts • 10 unsuccessful logins
Acceptance Criteria	The success ratio of all steps is 100%

Activity ID	**Integration_5**
Activity type	Benchmarking
Activity description	Evaluate the infrastructure communications trustworthiness. 1- Confirm communications between nodes, enforce state of the art encryption, preventing any tapping
Acceptance Criteria	Step 1 is successful

Activity ID	**Integration_6**
Activity type	Stress Test
Activity description	Evaluate the *persistence engine* performance levels and scalability. 1- Being all nodes online and 2 SL App nodes, with an automated script execute through SL Business Layer interface, 10, 20 and 100 simultaneous sessions doing: • 100 create actions over: Schedules; Users • 100 edit actions over: Schedules; Users • 100 delete actions over: Schedules; Users • 10 successful logins & logouts 2- 10 unsuccessful logins being *f* (tolerated faults) nodes unreachable and 2 SL App nodes, with an automated script execute through SL Business Layer interface, 10, 20 and 100 simultaneous sessions doing: • 100 create actions over: Schedules; Users • 100 edit actions over: Schedules; Users • 100 delete actions over: Schedules; Users • 10 successful logins & logouts • 10 unsuccessful logins 3- Being *f* nodes compromised (reachable but with un-synched data) and 2 SL App nodes, with an automated script execute through SL Business Layer interface, 10, 20 and 100 simultaneous sessions doing: • 100 create actions over: Schedules; Users

	• 100 edit actions over: Schedules; Users • 100 delete actions over: Schedules; Users • 10 successful logins & logouts • 10 unsuccessful logins 4- Being all nodes online and 2 SL App nodes, with an automated script execute through SL Business Layer interface, 10, 20 and 100 simultaneous sessions doing (while doing it, cut the cord to *f* nodes): • 100 create actions over: Schedules; Users • 100 edit actions over: Schedules; Users • 100 delete actions over: Schedules; Users • 10 successful logins & logouts • 10 unsuccessful logins
Acceptance Criteria	The average response time of all steps is less than 100ms.

Activity ID	**Integration_7**
Activity type	Stress Test
Activity description	Evaluate the *display cache* performance levels and scalability. 1- Being all *persistence* nodes online and 2 SL App nodes, with an automated script execute through SL Business Layer interface, 10, 20 and 100 simultaneous sessions doing: • 1 add consumption stats to cache • 100 read consumption stats from cache • 1 update consumption stats to cache • 100 read consumption stats from cache
Acceptance Criteria	The average response time of all steps is less than 10ms.

3.4.2.2.2 Trusted Object Manager

Activity ID	**Trusted_O_1**
Activity type	Proof of concept
Activity description	TVD management from TOM 1- Create TVDs and deploy Smart Lighting System VMs in TVDs on TrustedServer. 2- check if corresponding PKI is properly deployed 3- Try to access from within the tvd to a resource outside the tvd boundaries 4- Try to access from outside to a resource into the tvd boundaries
Acceptance Criteria	Activity is passed if • point 2 show a properly deployment

	• Point 3 fails • Point 4 fails

Activity ID	**Trusted_O_2**
Activity type	Proof of concept
Activity description	Remote management access 1- Access remotely to TOM management system 2- Stop Smart Lighting VMs 3- Check that VM's are not accessible by non-authorized people, preventing confidentiality
Acceptance Criteria	Activity is passed if • point 3 pass

Activity ID	**Trusted_O_3**
Activity type	Proof of concept
Activity description	Operate TrustedServer via TOM and TrustedChannel 1- Manipulate data on server and try to boot. This should fail
Acceptance Criteria	Activity is passed if • Activity at point 1 fails

3.4.2.2.3 Trusted Server

Activity ID	**Trusted_S_1**
Activity type	Proof of concept
Activity description	Inspect that there is no root account on TrustedServer Inspect an TrustedServer and ensure that there is no active root account where an administrator could log in.
Acceptance Criteria	Activity is passed if • There is no active root account at administrator login point

Activity ID	**Trusted_S_2**
Activity type	Proof of concept
Activity description	Test Secure Boot of Trusted Server 1- Boot integer server, this should work properly. 2- Manipulate data on server and try to boot. This should fail.

Acceptance Criteria	Activity is passed if • Activity at point 2 fails

Activity ID	Trusted_S_3
Activity type	Proof of concept
Activity description	Test local disks of TrustedServer 1- Run TrustedServer according to the use cases on D2.4.2 chapter 4.4.1.2 2- Check if data on local disk is properly encrypted
Acceptance Criteria	Activity is passed if • Activity at point 2 shows encrypted data
References Documents:	(Deliverable D2.4.2, 2012)

3.4.2.2.4 Trusted Channel

Activity ID	Trusted_C_1
Activity type	Proof of concept
Activity description	1- Establish trusted channel with Smart Lighting System VMs and check that data is properly encrypted
Acceptance Criteria	Activity is passed if • Activity at point 1 demonstrate the encryption of transferred data

Activity ID	Trusted_C_2
Activity type	Proof of concept
Activity description	1- establish trusted channel with authentic communication partners of Smart Lighting System appliance, check if communication works 2- try to establish channel with non-authentic partner, check that communication is refused
Acceptance Criteria	Activity is passed if • Activity at point 1 demonstrate the encryption of transferred data + the correct communication among VMs • Activity at point 2 fails

3.4.2.2.5 State Machine Replication (BFT-SMaRt)

Activity ID	BFT-SMART_1
Activity type	Proof of concept
Activity description	1- Deploy Smart Lighting System VMs into TClouds infrastructure 2- Insert data in a key value store and query the server to guarantee that the data has been correctly saved
Acceptance Criteria	Activity is passed if • Point 2 is confirmed

Activity ID	BFT-SMART_2
Activity type	Proof of concept
Activity description	Test the protocol in a faulty non-leader replica 1- By using the Smart Lighting System appliance, continuously store and query data, checking that the queried data is always as expected. 2- Turn off a replica 3- Switch on the replica after a certain time
Acceptance Criteria	Activity is passed if • Point 1 never report an error while performing the disconnection of a replica

Activity ID	BFT-SMART_3
Activity type	Proof of concept
Activity description	Test the protocol in a faulty non-leader replica 1- By using the Smart Lighting System appliance, continuously store and query data, checking that the queried data is always as expected. 2- Turn off a replica 3- Switch on the same replica after a certain time 4- Switch off another replica
Acceptance Criteria	Activity is passed if • Point 1 never report an error while performing the disconnection of a replica • At point 7 the system is capable of responding to request by using the data it received from the state transfer protocol.

Activity ID	**BFT-SMART_4**
Activity type	Proof of concept
Activity description	Test the protocol in a faulty leader replica 1- By using the Smart Lighting System appliance, continuously store and query data, checking that the queried data is always as expected. 2- Turn off a leader replica
Acceptance Criteria	Activity is passed if • Point 1 never report an error while performing the disconnection of a replica

Activity ID	**BFT-SMART_5**
Activity type	Proof of concept
Activity description	Test the leader change protocol and state transfer protocol 1- By using the Smart Lighting System appliance, continuously store and query data, checking that the queried data is always as expected. 2- All replicas, including the leader are switched on and off in a round robin fashion
Acceptance Criteria	Activity is passed if • Point 1 never report an error while performing the disconnection of a replica

3.4.2.2.6 Simple Key/Value Store

Activity ID	**Simple_KVS_1**
Activity type	Benchmarking
Activity description	Use two identical copy of the same VM-Xen-based of the Smart Lighting System appliance. 1- Place the original memcached installation in the first VM 2- Place the TClouds Haskell memcached in the second VM 3- Turn on the first VM and off the second and run an resource intensive core to stress the memcached feature and record the results 4- Switch the VMs and run the same test stressing the TClouds memcached feature 5- Compare the results
Acceptance Criteria	Activity is passed if • TClouds feature has better performances

Chapter 4 Appendix

4.1 Mapping on prototype subsystems and old D3.3.3 requirements

In this chapter are mapped the actual requirements of this document with the requirements of the old D3.3.3 deliverable For each requirement is described the subcomponent that will satisfy the requirement and, where applicable, the old requirements used in the first version of D3.3.3.

LREQ1

- Secure Block Storage + Secure VM instances
- LogService
  - HL1 – LogService must be capable of recording many log entries and to provide a view on a subset of the log entries that satisfy a particular query. Moreover, it must be capable to persistently store log entries for long period of time
- Resilient Object Storage (DepSky)
  - HL4 – Guarantee confidentiality of data stored. Data can’t be read from a single cloud provider
  - HL5 – Build diversity protocol to be able to store data in different clouds from different vendors
- Trusted Server
  - TS3 – Confidentiality of data stored on local disks

  TS1 – Remote Management via trusted channel, no root account for cloud administrators

LREQ2

- Resource efficient BFT (Cheap-BFT)
  - HL1 – Cheap BFT must be able to tolerate one or more arbitrary faults in the network or replica hardware. The service Running on top of it may not be affected by the fault
- Resilient Object Storage (DepSky)
  - HL4 – Guarantee confidentiality of data stored. Data can’t be read from a single cloud provider
  - HL5 – Build diversity protocol to ba able to store data in different clouds from different vendors
- Trusted Server
  - TS2 – Secure Boot: only an integer system is booted
- State machine replication (BFT-SMART)
  - HL1 – Define a resilient middleware that provides an adaptable suite of protocols appropriate for a range of applications running on CoC
  - HL2 – Offer tolerance to byzantine and crash faults for replicated services

LREQ3

- LogService
  - HL1 – LogService must be capable of recording many log entries and to provide a view on a subset of the log entries that satisfy a particular query.

Moreover, it must be capable to persistently store log entries for long period of time

- ACaaS
  - R1 – geographical restrictions: you can define which location the VM can run on, and the trusted scheduler will enforce this requirement.
  - R2 – multi-tenancy problem: you can request that the users who cannot share the physical resources with, or if you wanted a dedicated physical server to host your VM.
  - R3 – Remote attestation
- Trusted Object Manager (TOM)
  -

LREQ4

- LogService
- Resilient Object Storage (DepSky)
  - HL4 – Guarantee confidentiality of data stored. Data can't be read from a single cloud provider
  - HL5 – Build diversity protocol to be able to store data in different clouds from different vendors

LREQ5

- LogService
  - HL1 – LogService must be capable of recording many log entries and to provide a view on a subset of the log entries that satisfy a particular query. Moreover, it must be capable to persistently store log entries for long period of time
  - HL3 – Log Service should provide the Forward Integrity security property. This important property guarantees that if an attacker succeeds in compromising the log system, he cannot modify log entries collected before his attack without being noticed
- RemoteAttestation
  - HL2 – Allow cloud Administrator to specify the integrity level for the physical host on which his virtual machines will be deployed
- Trusted Object Manager (TOM)
  - TOM1 – User Centric Management of security Policy via web interface

AHSECREQ1

- Secure Block Storage + Secure VM instances
- Resilient Object Storage (DepSky)
  - HL4 – Guarantee confidentiality of data stored. Data can't be read from a single cloud provider
  - HL5 – Build diversity protocol to be able to store data in different clouds from different vendors

AHSECREQ2

- Resource efficient BFT (Cheap-BFT)
  - HL1 – Cheap BFT must be able to tolerate one or more arbitrary faults in the network or replica hardware. The service Running on top of it may not be affected by the fault
- Secure Block Storage + Secure VM instances
- Resilient Object Storage (DepSky)
  - HL4 – Guarantee confidentiality of data stored. Data can't be read from a single cloud provider

  - HL5 – Build diversity protocol to ba able to store data in different clouds from different vendors

AHSECREQ3

- Resource efficient BFT (Cheap-BFT)
  - HL1 – Cheap BFT must be able to tolerate one or more arbitrary faults in the network or replica hardware. The service Running on top of it may not be affected by the fault

AHSECREQ4

- Resource efficient BFT (Cheap-BFT)
  - HL1 – Cheap BFT must be able to tolerate one or more arbitrary faults in the network or replica hardware. The service Running on top of it may not be affected by the fault
- Resilient Object Storage (DepSky)
  - HL4 – Guarantee confidentiality of data stored. Data can't be read from a single cloud provider
  - HL5 – Build diversity protocol to be able to store data in different clouds from different vendors

AHSECREQ5

- Resource efficient BFT (Cheap-BFT)
  - HL1 – Cheap BFT must be able to tolerate one or more arbitrary faults in the network or replica hardware. The service Running on top of it may not be affected by the fault

AHSECREQ6

- LogService
  - HL3 – Log Service should provide the Forward Integrity security property. This important property guarantees that if an attacker succeeds in compromising the log system, he cannot modify log entries collected before his attack without being noticed
- RemoteAttestation
  - HL1 – Allow cloud User to specify the integrity level for the physical host on which his virtual machines will be deployed
  - HL2 – Allow cloud Administrator to specify the integrity level for the physical host on which his virtual machines will be deployed

AHSECREQ7

- LogService
  - HL4 –Since the log entries contain sensitive information about the usage of a certain system, log Service must be capable to mediate every access in order to prevent leakage
- RemoteAttestation
  - HL1 – Allow cloud User to specify the integrity level for the physical host on which his vistual machines will be deployed
  - HL2 – Allow cloud Administrator to specify the integrity level for the physical host on which his virtual machines will be deployed

AHSECREQ8

- Resource efficient BFT (Cheap-BFT)
  - HL1 – Cheap BFT must be able to tolerate one or more arbitrary faults in the network or replica hardware. The service Running on top of it may not be affected by the fault

AHPRIVREQ1

ASSECREQ1

- Trusted Server
- Simple Key/Value Store (memcached)
- Trusted Object Manager (TOM)
- Trusted Management Channel
- TS + TOM + TMC
    - R3 – Mitigate risk of insider attack by a new trust model…

ASSECREQ1

- Log Service

ASSECREQ3

- State machine replication (BFT-SMART)
    - LL2 – Guarantee confidentiality of data stored in the CoC
- Trusted Object Manager (TOM)
    - TOM2 – Secure PKI management for TVDs…

ASSECREQ4

- State machine replication (BFT-SMART)
    - LL1 – Leverage availability of data through replication

ASSECREQ5

- State machine replication (BFT-SMART)
    - HL1 – Define a resilient middleware that provides an adaptable suite of protocols appropriate for a range of applications running on CoC
- Trusted Management Channel
    - TC1 – Confidentiality and integrity of communication
    - TC2 – Authentication of communication partners

ASSECREQ6

- Simple Key/Value Store (memcached)
    - HL1 – Simple caching service that runs on top of most cloud providers which is resource-efficient and secure, in order to speed up frequent, computation intensive operations

NOTE:
As clearly is described in the list above, AHPRIVREQ1 have no subcomponents that satisfy it.
This is due to the fact that the requirements list has been prepared in early stages of the development of TClouds Infrastructure. By understanding better the actual needs of A3 use cases and A2 technical capabilities we found that:

- *AHPRIVREQ1 is a requirement that cannot be satisfied by TClouds Infrastructure since it is clearly a requirement that can be satisfied only at platform level (PaaS), meanwhile the main infrastructure aims to build services at IaaS level.*

Healthcare Surveys

4.1.1 Survey for Developers

The survey is combined with a presentation that can be found as starting the survey at the link below

The survey itself is available online at: http://tclouds.eservices4life.org/67421/lang-en

Following, the questions placed into the survey:

QUESTION 1:

If you were using a cloud enabled platform to log, save and share health personal data, how important would the following topics be to you? Please number each box in order of preference from 1 to 4

□Availability 24/7 of health information into the system

□Security of health information

□Transparency and control of third party application accessing users' health information

□Security of developer's data

TO FIX THE CONCEPTS:

Availability 24/7 of health information into the system: the platform guarantees that its services and users data are always available assuring, at Terms of Service level, that there will be no downtime (thus, 100% uptime).

Security of health information: all user's data are saved into the platform in respect of the highest security standards like data cryptography and reduction of data value concentration on every single physical node.

Transparency and control of third party application accessing users' health information: the platform keeps track of each activity executed: from data transfer to privacy policy changes. Transparency means to allow data owner to have detailed report about the usage of its data. Control means to give to the user the ability to share his data respecting his privacy as well as enterprise policies (in case of on the data are applied legal restriction)

Security of developer's data: when we refer to manage data with high security and transparency, we are not only referring to final user's data, but also to developer's data (such as account data and app details)

QUESTION 2

In scope of "Transparency and trust in other parties applications", how important are the following topics to you? Please number each box in order of preference from 1 to 5

□Sentence1: "The platform must log the CRUD (Create, Read, Update, Delete) activity of third party applications"

□Sentence2: "It must be possible for a developer to audit all the activity that the application is doing on the platform"

□Sentence3: "All log are depersonalized and does not allow developer to know the identity of who performed a certain activity"

□Sentence 4: App's user Health information can be used (under user consensus) in a depersonalized form to extract meaningful data (such as for research or marketing purposes)

□Sentence 5: An application should not being able to provide/share user health information to other third parties (without user's consensus)

TO FIX THE CONCEPTS:

The platform must log the CRUD (Create, Read, Update, Delete) activity of third party applications: all the activity performed into the platform are logged. When an application uses the platform's API all the activity of data sharing are logged as well. Many are the details that are logged, among them:

The user performing the request

The application used

The type of action performed

The data transferred

The owner of the data

It must be possible for a developer to audit all the activity that the application is doing on the platform: to allow the platform to log all the activity has the advantage the opportunity to have many different auditing options like analysis for debugging or marketing purposes.

All log are depersonalized and does not allow developer to know the identity of who performed a certain activity: to maintain data privacy, all the audits does not include user data that allow to hail from him.

App's user Health information can be used (under user consensus) in a depersonalized form to extract meaningful data (such as for research or marketing purposes): auditing and data mining can be done only under users consensus.

An application should not being able to provide/share user health information to other third parties (without user's consensus): self-explicative

QUESTION 3:

In scope of "Availability and flexibility of your data and application", how important are the following topics to you? Please number each box in order of preference from 1 to 2

□Sentence1: "My third party application should always have access to the platform's API. The service should be available 24/7 with no downtime."

□Sentence2: "Applications have the chance to save locally data retrieved from the system."

□Sentence3: "Data should always be available through duplication and distribution"

TO FIX THE CONCEPTS:

My third party application should always have access to the platform's API. The service should be available 24/7 with no downtime: the service to exchange data between the platform and the applications is guaranteed to have no downtime (100% uptime)

Applications have the chance to save locally data retrieved from the system: may happen that the connection to the platform is not available. To increase efficiency and system responsiveness big application (those with thousands of users connected, such as an hospital's clinical record management) needs to adopt techniques of local caching of the data.

QUESTION 4:

In scope of "Security of my data", how important are the following topics to you? Please number each box in order of preference from 1 to 3

□Sentence 1: "When deleting the developer account, all my (developer) details must be deleted"

□Sentence 2: "When a developer deletes an app, all the data of the given app should be deleted (not the health data, but only the data related to the app itself)"

□Sentence3: "When a developer deletes an app. all the health data generated by the app should be deleted as well"

TO FIX THE CONCEPTS:

When deleting the developer account, all my (developer) details must be deleted: Delete all account data means remove completely the information from the databases that refers to that specific user. Thus, it is not simply marked as "deleted". In this question is not considered deletion policies of backup data.

When a developer deletes an app, all the data of the given app should be deleted (not the health data, but only the data related to the app itself): same as the previous question, but with reference to the app data saved into the system.

When a developer deletes an app. all the health data generated by the app should be deleted as well: in this case is considered the removal of all the data, included the health data of the users that the application has generated. User, hence, will experience a removal of all their data collected while using the app.

QUESTION 5:

In the scope of “Security of health information". Please number each box in order of preference from 1 to 3

□Sentence 1: I must be able to define the minimum policy requirements that an app user has to accept in order to use the application properly.

□Sentence 2: Health information should be always encrypted and decryption keys are not in developers hand

□Sentence3: "Local storage is encrypted and decryption keys resides into the platform itself. The developer uses a specific library provided by the system in order to be able to decrypt and use the information"

□Sentence4: “user's data must be saved in location that are compliant with the legislation of their country”

TO FIX THE CONCEPTS:

I must be able to define the minimum policy requirements that an app user has to accept in order to use the application properly: when an user decides to use an app he must accept a series of policies that allows the application to access to (or save) a subset of the user's data necessary to allow the app to work (similarly as when using an app in one of the most famous app market (see Android/Apple app markets)

Health information should be always encrypted and decryption keys are not in developers hand: data inside the platform are all encrypted. Decryption keys are maintained into the platform and are provided where needed.

Local storage is encrypted and decryption keys resides into the system itself. The developer uses a specific library provided by the system in order to be able to decrypt and use the information: the application has access to the data through a specific library provided by the platform. The library manages the communication between the platform and the application and the local data storing.

User's data must be saved in location that are compliant with the legislation of their country: TPaaS takes care of all the data saved into it. Health information are very sensitive data that has to respect specific privacy and security rules. This can be done by enforcing the "geo-localization" of the data. Assuring that health data will never be stored in countries that allows data manipulation non allowed by the legislation of the user's country

QUESTION 6:

Score the sentences, Please number each box in order of preference from 1 to 5

□Sentence1: You are interested in developing consumer application (related with PHR data)

□Sentence2: You are interested in developing professional application (related with EHR data)

□Sentence3: You are interested in connect devices to the platform

□Sentence4: Build an application that is able to get user health information that comes from other applications/devices other than yours

□Sentence5: Build an application knowing that the data that the app saves into the platform can be shared with other applications

4.1.2 Survey for Patients

The survey is combined with a presentation that can be found as starting the survey at the link below.

The survey itself is available online at: http://tclouds.eservices4life.org/65519/lang-en

Following, the questions placed into the survey:

QUESTION 1:

If you were using a web-based enabled service to log, save and share your personal health information, how important would the following topics be to you?

Please number each box in order of preference from 1 to 3

□Availability 24/7 of my health information

□Security of my health information (such as sharing rules and data encryption)

□Transparency and control of third parties accessing my information (third parties could be doctors, applications, friends and family)

QUESTION 2:

In scope of "Transparency and control of third parties accessing your information", how important are the following topics to you? Please number each box in order of preference from 1 to 6

□Sentence1: It must be possible for me to hide some information from my doctor (diary, notes)

□Sentence2: It must be possible to add and remove persons who are allowed to access to my information.

□Sentence3: The system must show who (and when) has been viewing or changing my health information

□Sentence4: The system must show who (and when) has been viewing or changing the information of someone else I am allowed to access to

□Sentence5: It must be visible to my doctor, when I have changed my information that I shared with him

□Sentence6: I would be happy to give my data anonymized to third parties.

TO FIX THE CONCEPTS:

It must be possible for me to hide some information from my doctor: You are in charge to take care of your data and you can decide which privacy policies adopt in order to show/hide any data to anyone.

It must be possible to add and remove persons who are allowed to access to my information: Manage your privacy policies means to decide, who has access to the data and which data he's allowed to access to. You can then be able to modify this privacy policies easily through the web interface of the platform.

The system must show who (and when) has been viewing or changing my health information: If someone has accessed to your data you need the chance to know it. TPaaS health platform is able to provide you an overview of who had access to your data, when and for which purpose.

The system must show who (and when) has been viewing or changing the information of someone else I am allowed to access to: Imagine you can see health data of one of your parents. If someone (e.g. a doctor) has access that data and add/removes/modify some information, you should know it.

It must be visible to my doctor, when I have changed my information that I shared with him: self-explicative

QUESTION 3:

In scope of "Availability 24/7 of my health information", how important are the following topics to you? Please number each box in order of preference from 1 to 7

□Sentence1: All my health information must be always available to my doctor

□Sentence2: Only the most important health information must be always be available to my doctor

□Sentence3: All my health information must always be available to me

□Sentence4: The third party application I use to enter, view and edit my health information should always have access to my information on the service

□Sentence5: If the service is not available, then the third party application should being able to work anyway with a local copy of my health information.

□Sentence6: There must always be enough space to hold my data.

□Sentence7: The loading time of a page in the apps I use has to be acceptable (eg. No more than 5 seconds)

QUESTION 4:

In scope of "Security of my data", how important are the following topics to you? Please number each box in order of preference from 1 to 5

□Sentence1: My data must be saved in location that are compliant with the legislation of my country

□Sentence2: My data must be safe from attackers and data leakage

□Sentence3: If an attacker is able to steal my health information, he can't read it anyway because he need decryption keys in order to read it

□Sentence4: If I want I have to be able to delete my data (no copies are maintained into the system)

□Sentence5: If I want to delete some health information that cannot be removed for legal issues (e.g. clinical data produced by an hospital), the system should stop me.

TO FIX THE CONCEPT:

My data must be saved in location that are compliant with the legislation of my country: TPaaS takes care of all the data saved into it. Health information are very sensitive data that has to respect specific privacy and security rules. This can be done by enforcing the "geo-localization" of the data. Assuring that health data will never be stored in countries that allows data manipulation non allowed by the legislation of your country

My data must be safe from attackers and data leakage: with the same consideration of the previous point, TPaaS leverages it storage capabilities to TClouds technology. This technology is proving to be resilient to serious attacks and data leakage becomes extremely unlikely to happen.

If an attacker is able to steal my health information, he can't read it anyway because they are encrypted: all the data saved are encrypted. This means that no one is able to read this data unless they have the decryption keys. Fortunately TClouds uses techniques that save decryption keys is different places than where the data is saved. This means that an attacker that has the chance to reach the data is not able to understand it since is completely encrypted and there are no decryption keys to look for.

If I want, I have to be able to delete my data (no copies are maintained into the system): often data deletion means to mark the data "as deleted" and it is not effectively deleted. In this case you have the chance to really delete any data and nothing is kept on the platform.

If I want, I have to be able to delete my data and chose if I want them permanently deleted or anonymously deleted: In this case the patient have the chance to decide how actually delete the data. By making data anonymous, the patient is no longer able to retrieve deleted data but it can be used for analytics (e.g. for medical research)

If I want to delete some health information that cannot be removed for legal issues (e.g. clinical data produced by an hospital), the system should stop me: self-explicative

QUESTION 5:

Please rank the following sentences. Please number each box in order of preference from 1 to 6:

□Sentence1: I should been able to print directly from the web-based service my health reports

□Sentence2: It must be possible to change my data (e.g. medicine intake logs) on a later moment, for example when I forgot to enter it, or discover a mistake.

□Sentence3: If I want I have to be able to export my data to take it into another service

□Sentence4: I am willing to give my anonymous health information for scientific research

□Sentence5: I am willing to give my anonymous health information for government policies

□Sentence6: I am willing to give my anonymous health information for marketing research

4.1.3 Survey for Doctors

The survey is combined with a presentation that can be found as starting the survey at the link below.

The survey itself is available online at: http://tclouds.eservices4life.org/28211/lang-en

Following, the questions placed into the survey:

QUESTION 1:

If you were using an internet platform to log, save and share your patients' data, how important would the following topics be to you? Please number each box in order of preference from 1 to 3

□Availability 24/7 of my patients' health data

□Security of my patients' health data

□Transparency and control of third parties accessing my patient's information (third parties could be doctors, applications, friends and family)

QUESTION 2:

In scope of "Transparency and control of third parties accessing Patient's health information", how important are the following topics to you? Please number each box in order of preference from 1 to 4

□Sentence1: It must be possible for my patient to hide health information from me.

□Sentence2: It must be visible to me, when my patient has changed his/her health information

□Sentence3: The system must show who (and when) has been changing the data I am allowed to access

□Sentence4: It must be possible for my patient to audit access I did to his/her health information

TO FIX THE CONCEPTS:

It must be possible for my patient to hide health information from me: Patients are in charge to take care of their data and can decide which privacy policies adopt in order to show/hide any data to anyone.

It must be visible to me, when my patient has changed his/her health information: may happen that clinical data have some errors. Patients, thus, have the chance to fix them. Changing history is available and doctors may have the chance to see either the original document and the modified one.

The system must show who (and when) has been changing the data I am allowed to access: you, as a doctor, have access to a various amount of data for each patient (either data that you have produces and data you did not). If someone else updates this data, you should be advised by the system, in order give you the opportunity to easily check what's new to your patient and, if necessary, take action.

It must be possible for my patient to audit access I did to his/her health information: patients have the chance to see all the access that has been made to his/her data. This means that the activity of a doctor accessing to his patients' data is recorded and shown to the patient.

QUESTION 3:

In scope of "Availability 24/7 of your patients' data", how important are the following topics to you? Please number each box in order of preference from 1 to 6

□Sentence1: The loading time of a page the apps I use, may not be more than 5 seconds

□Sentence2: The patient's health information must always be available to me

□Sentence3. If the platform is not available, then the third party application should being able to work anyway with a local copy of my patient's health information

□Sentence4: There must always be enough space to hold my patients’ data

□Sentence5: The patient’s data must always be available to my patient

□Sentence6: Given a patient, I must be able to specify which key info should be available 24/7 for him/her

TO FIX THE CONCEPTS:

The loading time of a page the apps I use, may not be more than 5 seconds: studies on usability show that the average time that a person is willing to wait is 5 seconds.

The patient’s health information must always be available to me: the platform should be reliable. And when a doctor access to a patient's health data, he don't have to experience out of service. Health information must be always available at any time.

If the platform is not available, then the third party application should being able to work anyway with a local copy of my patient's health information: may happen that the connection to the platform is interrupted, this however, should not block doctors work. The computer application that the doctor uses should be able to save locally all the necessary data to work while disconnected.

There must always be enough space to hold my patients’ data: self-explicative

The patient’s data must always be available to my patient: self-explicative

Given a patient, I must be able to specify which key info should be available 24/7 for him/her: There are some health data for each patient that are data that should be always available to any doctor (e.g. allergies, blood type, chronic conditions...) 24/7. This information are accessible anytime for emergency purposes.

QUESTION 4:

In scope of "Security of my patient's data", how important are the following topics to you? Please number each box in order of preference from 1 to 4

□Sentence1: My patient's data must be saved in location that are compliant with the legislation of my country

□Sentence2: My patient’s data must be safe from attackers and data leakage

□Sentence3: If an attacker is able to steal health information, he can’t read them because they are encrypted.

□Sentence4: If patients want they have to be able to delete their data (no copies are maintained into the system)

TO FIX THE CONCEPTS:

My patient's data must be saved in location that are compliant with the legislation of my country: TPaaS takes care of all the data saved into it. Health information are very sensitive data that has to respect specific privacy and security rules. This can be done by enforcing the "geo-localization" of the data. Assuring that health data will never be stored in countries that allows data manipulation non allowed by the legislation of the patient's country

My patient’s data must be safe from attackers and data leakage: with the same consideration of the previous point, TPaaS leverages it storage capabilities to TClouds technology. This technology is proving to be resilient to serious attacks and data leakage becomes extremely unlikely to happen.

If an attacker is able to steal health information, he can’t read them because they are encrypted: all the data saved are encrypted. This means that no one is able to read this data unless they have the decryption keys. Fortunately TClouds uses techniques that save decryption keys is different places than where the data is saved.

This means that an attacker that has the chance to reach the data is not able to understand it since is completely encrypted and there are no decryption keys to look for.

If patients want, they have to be able to delete their data (no copies are maintained into the system): often data deletion means to mark the data "as deleted" and it is not effectively deleted. In this case you have the chance to really delete any data and nothing is kept on the platform.

If patients want, they have to be able to delete their data and chose if they want it permanently deleted or anonymously deleted: In this case the patient have the chance to decide how actually delete the data. By making data anonymous, the patient is no longer able to retrieve deleted data but it can be used for analytics (e.g. for medical research)

4.2 Smart Lighting System Survey

The survey itself is available online at: http://www.surveymonkey.com/s/8KWLN2G

The Smart Lighting System survey is unique for the three SLS' stakeholders (Municipalities, Utilities, Vendors). It will be performed by EDP and mainly via direct interviews.

Following, the questions placed into the survey:

1. Trustworthy audit

"Smart Lighting actions (application access; create, update and delete data) must be fully audited, and accessible only to privileged users."
In a scale of 1 to 10, please select the option that better fits your concerns.

Please consider the following reference levels:
1 - There is only one administrator access, which is controlled;
5 - Actions in my system must be traceable;
10 - System must be full audited.

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

2. Trustworthy infrastructure

"The hosting infrastructure must prevent intrusions."
In a scale of 1 to 10, please select the option that better fits your concerns.

Please consider the following reference levels:
1 - My infrastructure could be hosted outside of my company but should be implemented with access control;
5 - My infrastructure must be isolated from the Internet with access control;
10 - My infrastructure must be isolated from the Internet and administrated only by me.

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

3. Trustworthy Persistence Engine

"The persistence engine must prevent intrusions and ensure confidentiality, integrity and availability."
In a scale of 1 to 10, please select the option that better fits your concerns.

Please consider the following reference levels:
1 - Security of my application is not important to me;
5 - My application implements access control;
10 - My application is administrated only by me.

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

4. Resilient

"The Smart Lighting System must be fault-tolerant at infrastructure and persistence level."
In a scale of 1 to 10, please select the option that better fits your concerns.

Please consider the following reference levels:
1 - My system should stop if it is compromised;
5 - My system must still operate, possibly at a reduced level, when some part fails;
10 - The system does not stop and it is able to retain its integrity while damaged.

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

5. Trustworthy communications

"Communications between a client and the Smart Lighting System must prevent data from being altered by using adequate security mechanisms."
In a scale of 1 to 10, please select the option that better fits your concerns.

Please consider the following reference levels:
1 - The communication should be secure but availability is more important for my organization;
5 - My system should ensure data is not altered by using adequate security mechanisms;
10 - My system must protect sensitive information by enabling computations with encrypted data and protect users from malicious behaviors by enabling validation of the computation result.

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

6. High performance & Scalable

"The Smart Lighting System must have near-realtime performance, and able to scale on increased load."
How long can my company operate without access to cloud data and services?

○ Less than 10 seconds
○ Between 10 seconds and 1 minute
○ Between 1 and 10 minutes
○ Between 10 minutes and 1 hour
○ It is not an issue

7. High performance & Scalable

"The Smart Lighting System must have near-realtime performance, and able to scale on increased load."
In a scale of 1 to 10, please select the option that better fits your concerns.

Please consider the following reference levels:
1 - My system does not change as much and scalability is not an issue.
5 - My system is growing at a constant rate; therefore cloud computing is a possible solution.
10 - The growth of my system is unpredictable and the cloud computing model is attractive because of its cost-effectiveness.

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

8. “The data in the cloud should be correct, consistent, accessible and high quality.”
Regarding the previous sentence, please choose the sentence that better fits your concerns.

- ○ Protect the cloud infrastructure in order to prevent intrusions
- ○ The system must still operate, possibly at a reduced level, when some part of fails. The system does not stop and is able to retain its integrity while damaged.

9. "Securing integrity of data in communications involves the use of methodologies that may compromise availability. However, there are situations in which availability is of most importance and those methodologies cannot be used."
Regarding the previous sentence, please choose the sentence that better fits your concerns.

- ○ My system should ensure the integrity of the data and provide proof that the data is transmitted in a secured manner even when it compromises availability.
- ○ The availability is one of the most important issues and it should not be compromised. My system must have near real-time performance even if that compromises integrity at communication level.

10. “Security efforts to assure confidentiality, integrity and availability can be divided into those oriented to prevention and those focused on detection. The balance between prevention and detection depends on the circumstances and the available security technologies.”
Regarding the previous sentence, please select Yes or No.

- ○ Yes.
- ○ No.

Chapter 5 References

C2FS. (s.d.). Tratto da https://svn.tclouds-project.eu/trunk/ActivityA2-TrustedCloudPlatform/Documents/A-ActivityPapers/TC-WP2_2-A10r01-C2FS/c2fs.pdf

Deliverable 2.2.1. (2010). Tratto da http://www.tclouds-project.eu/downloads/deliverables/TC-D2.2.1_Preliminary_Architecture_for_Middleware_for_Adaptive_Resilience_M12.pdf

Deliverable D2.1.2. (2012, September). Tratto da http://www.tclouds-project.eu/downloads/deliverables/TC-D2.1.2-Prelim-Mechanisms-Components-Single-Trusted-Clouds_M24.pdf

Deliverable D2.3.2. (s.d.). Tratto da http://www.tclouds-project.eu/downloads/deliverables/TC-D2.3.2-Components-Architecture-Security-Configuration-Privacy-Mgt_M24.pdf

Deliverable D2.4.2. (2012, September). Tratto da http://www.tclouds-project.eu/downloads/deliverables/TC-D2.4.2_Initial-Component-Integration_M24-V1.1.pdf

Depsky. (2011). Tratto da http://www.gsd.inesc-id.pt/~mpc/pubs/eurosys219-bessani.pdf

Intel Open Attestation SDK. (s.d.). Tratto da https://github.com/OpenAttestation/OpenAttestation

Logging handlers. (s.d.). Tratto da http://docs.py thon.org/2/library/logging.handlers.html

Resource Efficient Byzantine Fault Tolerance. (2012). Tratto da http://doi.acm.org/10.1145/2168836.2168866

TClouds factsheet - Log as a Service. (2013, April). Tratto da http://www.tclouds-project.eu/downloads/factsheets/tclouds-factsheet-05-logging.pdf

TClouds factsheet 03 - Cryptography. (n.d.). Retrieved from http://www.tclouds-project.eu/downloads/factsheets/tclouds-factsheet-03-cryptography.pdf

TClouds factsheet 09 Cheap BFT. (2013, April). Tratto da http://www.tclouds-project.eu/downloads/factsheets/tclouds-factsheet-09-cheap.pdf