D1.1.4 – Version 2

Final Scenario Framework

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

Deliverable type:	Report
Deliverable reference number:	ICT-257243 / D1.1.4 / 2.0
Activity and Work package contributing to the deliverable:	Activity 1 / WP1.1; WP1.3, Activity 2 / WP2.1, WP2.2, WP2.3; Activity 3 / WP3.1, WP3.2
Due date:	March 2012 – M18
Actual submission date:	2nd April 2012

Responsible organisation:	UMM
Editor:	Ruediger Glott
Dissemination level:	Public
Revision:	2.0

Abstract:	This deliverable is an update of the deliverable D1.1.4 that was submitted in September 2011 (M12 of the project). It provides a framework for the development of cloud computing scenarios that aim at current and future privacy and security issues of cloud computing from the perspective of business models and business processes. In this document, the concepts of business models and business model risks are discussed and the methodology for the overall scenario building process in Activity 1 is presented. After an overview of general cloud computing trends and their impact on the cloud computing ecosystem the two application

	scenarios of TClouds, home health care and public lighting, are considered from the viewpoint of business models and business model risks. After evaluating the scenarios from the business perspective, the implications of the TClouds platform architecture for business models and business model risks are considered and a first approach to relating business model risks to the 15 TClouds components that have been selected in Activity 2 for the TClouds prototype architecture (see D2.4.1) and to other privacy, security and resilience related decisions made in Activity 2 and Activity 3 is developed. Given the feedback loops between Activities 1, 2 and 3, this report is partly based on other project deliverables, as it relies, on the one hand, on the overall description and the detailed use cases of the two application scenarios in Activity 3 and, on the other hand, on the TClouds platform architecture that was developed in Activity 2. The contribution of Activity 1 consists of the identification of fundamental cloud computing trends and possible trajectories of cloud computing, and the risks aligned with them.
Keywords:	Cloud computing, cloud computing trends, healthcare, public lighting, business models, business model risks.

Editor

Ruediger Glott (UMM)

Contributors

Imad Abbadi (UOXF)
Marco Abitabile (HSR)
Miguel Areias (EDP)
Ilaria Baroni (HSR)
Johannes Behl (FAU)
Alysson Bessani (FFCUL)
Sören Bleikertz (IBM)
Sven Bugiel (TUDA)
Christian Cachin (IBM)
Emanuele Cesena (POL)
Miguel Correia (FFCUL),
Mina Deng (PHI)
Ruediger Glott (UMM)
Michael Gröne (SRX)
Thomas Groß (IBM)
Miguel Grossinho (EDP)
Kirsten Haaland (UMM)
Andreas Meiszner (UMM)
Marco Nalin (HSR)
Stefan Nürnberger (TUDA)
Michael Osborne (IBM)
Marcelo Pasin (FFCUL),
Milan Petkovic (PHI)
Gianluca Ramunno (POL),
Alberto Rodrigues (EFA)
Paulo Jorge Santos (EFA)
Norbert Schirmer (SRX)
Matthias Schunter (IBM)
Paolo Smiraglia (POL)
Klaus Stengel (FAU)
Paulo Viegas (EFA)
Davide Vernizzi (POL)

Disclaimer

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

Executive Summary

This deliverable is an update of the deliverable D1.1.4 that was submitted in September 2011 (M12 of the project). It provides a framework for the development of cloud computing scenarios that aim at current and future privacy and security issues of cloud computing from the perspective of business models and business processes.

In this document, the concepts of business models and business model risks are discussed and the methodology for the overall scenario building process in Activity 1 is presented.

After an overview of general cloud computing trends and their impact on the cloud computing ecosystem the two application scenarios of TClouds, home health care and public lighting, are considered from the viewpoint of business models and business model risks.

After evaluating the scenarios from the business perspective, the implications of the TClouds platform architecture for business models and business model risks are considered and a first approach to relating business model risks to the 15 TClouds components that have been selected in Activity 2 for the TClouds prototype architecture (see D2.4.1) and to other privacy, security and resilience related decisions made in Activity 2 and Activity 3 is developed.

Given the feedback loops between Activities 1, 2 and 3, this report is partly based on other project deliverables, as it relies, on the one hand, on the overall description and the detailed use cases of the two application scenarios in Activity 3 and, on the other hand, on the TClouds platform architecture that was developed in Activity 2. The contribution of Activity 1 consists of the identification of fundamental cloud computing trends and possible trajectories of cloud computing, and the risks aligned with them.

Updated Version (March 2012):

Overall, this document updates D1.1.4 as submitted in M12 of the project. The update pertains the following points that were not laid out explicitly or clearly enough in the previous version of D1.1.4:

- In chapter 1, the framework used in Activity 1 is explained
- Chapter 2 describes in more detail the general approach of Activity 1 towards business requirements and their match with Activity 2 and Activity 3, including examples of cloud-related business model risks.
- Chapter 4 refers to the further development of the approach in WP3.1 after year 1 of the project, which is laid out in D3.1.2, while the previous version of D1.1.4 referred to the approach followed in year 1 and described in D3.1.1. This change was made in order to keep coherence between Activity 1 and Activity 3.
- Chapters 4 and 5 describe the implications of the two application scenarios for business models in more detail than the previous version of D1.1.4
- Chapter 6 provides a description of the TClouds platform architecture and an evaluation of the role of the 15 privacy and security components of TClouds from a business perspective.
- The concluding chapter includes concrete recommendations for Activity 2 and Activity 3 to be provided to potential TClouds users.
- The results of the ongoing empirical work of Activity 1 will be documented in the Deliverables relating to the scenario workshop and in an update of D1.1.4 Version 3.0 in M22.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Chapter Authors:

Ruediger Glott (UMM), Kirsten Haaland (UMM), Andreas Meiszner (UMM)

1.1 Purpose

This deliverable aims at following objectives:

- It provides a framework for the development of cloud computing scenarios that aim at current and future privacy and security issues of cloud computing from the perspective of business models and business processes. This framework consists of following parts:
    - An explanation of the concepts of business models and business model risks that provide the foundation for the methodology for the scenario building
    - General cloud computing trends and their impact on the cloud computing ecosystem
    - A reference to the TClouds application scenario descriptions as provided by WP3.1 and WP3.2, evaluated with regard to their implications for business models and business model risks
    - A reference to the TClouds platform architecture and its implications for business models and business model risks
- It provides a concept of business models as the conceptual basis for the work in Activity 1 and the business-related evaluation of the TClouds cloud of clouds in Activity 3.
- It provides a first approach to relating business model risks to the 15 TClouds components that have been selected in Activity 2 for the TClouds prototype architecture (see D2.4.1) and to other privacy, security and resilience related decisions made in Activity 2 and Activity 3.
- It identifies general trends and trajectories of cloud computing and cloud scenarios. To this end, an explorative interview with an identity and access management (IAM) expert has been carried out in the starting phase of the project and extent market and ecosystem analyses have been evaluated (see also D1.1.1 and D1.3.1).
- It compares the two TClouds application scenarios (public lighting and home healthcare) to these generic trends and evaluates the concepts of these two application scenarios. For the latter purpose, a focus group (internal working group with an external expert in the public lighting scenario) and two expert talks (in the home healthcare scenario) have been carried out, piloting the identification of final scenarios through expert interviews and a scenario building workshop in year 2 of the TClouds project. The purpose of this approach is to evaluate where the two application pilots of the project stand as compared to other cloud computing implementations and strategies in the two sectors (energy supply and healthcare),

which complements the evaluation of these two scenarios in Activity 3 of the TClouds project.

Given the feedback loops between Activities 1, 2 and 3, this report is partly based on other project deliverables, as it relies, on the one hand, on the overall description and the detailed use cases of the two application scenarios in ACTIVITY 3 and, on the other hand, on the TClouds platform architecture that was developed in ACTIVITY 2. The contribution of ACTIVITY 1 consists of the identification of fundamental cloud computing trends and possible trajectories of cloud computing, and the risks aligned with them.

1.2 Outline of this Deliverable

The report is structured as follows: In chapter 3 we will describe the general approach of WP1.1. and WP1.3 towards the identification and evaluation of business requirements from cloud computing, in particular with regard to the two usage scenarios and the TClouds platform. Chapter 4, a general overview of trends in cloud computing ecosystems will be provided in order to update information that was given by ACTIVITY 1 in previous deliverables. Given the strong dynamics and volatility in the market, such an update is necessary in order to make sure that the evaluation of the two usage scenarios and the TClouds platform from a business perspective is appropriate. After the overview of generic trends, the two usage scenarios and the approach of ACTIVITY 2 towards security, privacy and resilience are laid out in the following three chapters (5-7). In chapter 8 we draw conclusions regarding business requirements from the TClouds application scenarios and platform and the ongoing empirical work (interviews and scenario building).

The results of the empirical work and of the scenario workshop will be documented in the deliverables directly related to the workshop and in an update of this deliverable.

Chapter 2

General Approach: Business Models and Business Model Risks

Chapter Authors:

Ruediger Glott (UMM), Kirsten Haaland (UMM), Andreas Meiszner (UMM)

2.1 Introduction

The general objective of WP1.1 and WP1.3 is to identify cloud computing risks from a business perspective, which shall feed in the further development of the two usage scenarios in ACTIVITY 3 and in the design and implementation of the TClouds platform in ACTIVITY 2. In the following we describe the two basic concepts for the approach of WP1.1 and WP1.3, 'business model' and 'business model risks'. In the concluding section, we will apply these concepts to the two usage scenarios and the platform architecture, as far as this is possible at the current state of work. Next to this, we will outline how this approach will be applied empirically in order to carry out interviews, gather cloud expertise through online discussions, and organize a scenario building workshop in order to identify relevant business model risks and viable scenarios for the TClouds cloud of clouds.

2.2 Business Models

The term 'business model' was introduced in the late 1950s but hardly used in publications until the 1990s, and only with the hype of the Internet it reached a first peak in 2000 (Horsti 2007). The term is used to capture the ways and means a business tries to achieve revenues. Since every business strives for value creation and revenues. there is no enterprise without a business model, regardless of whether or not a company can explicitly describe it (Teece 2010; Chesbrough 2006).

Enterprises operate under changing market conditions, i.e. demand, competition, technologies etc. tend to change over time (Teece 2010). Business models provide enterprises a strategic resource to adapt to these changing conditions. These reactions and adaptations to the specific context conditions of an enterprise make business models unique: two companies selling the same product on the market would always achieve different economic outcomes (Chesbrough 2010).

However, despite its long history and widespread usage, the term is not at all clear-cut. Many authors mean completely different things when using the term (Osterwalder 2004; Al-Debei & Avison 2010). One of the main reasons for this is that (business) economics did not provide a theoretical foundation of the concept of a business model (Teece 2010; Morris et al. 2005). Teece (2010) explains this shortcoming by the focus of economics on theoretical matters, whereas the business model concept aims at the solution of real world business problems and challenges. As a conclusion, Amit & Zott's (2001) finding that there is no commonly accepted or dominant theory or definition of business models holds still true.

A consequence of the lack of a single comprehensive theoretical concept of business models is that in practice business models are often conceptualized as a company-specific feature, such as Apple's iTunes model, or as a generic principle to generate revenues, such as the freemium model or the bricks and clicks model.

Academic conceptualization of the notion of "business model" often regard the interplay between product / service, the business actors, value creation and revenue sources (e.g. Timmers 1998; Osterwalder at al. 2005; Casadesus-Masanell & Ricart 2010; Zott & Amit 2010), others concentrate more on innovations and how to generate revenues from them (Chesbrough & Rosenbloom 2002), emphasize the sort of transaction partners and channels (B2B, B2C, B2G, P2P) [19], or the firm's position in the value chain and revenue (Schlachter 1995; Rappa 2004).

The problem of these definitions is that they emphasize different aspects that may be relevant for business models but do not systematically examine how business models are composed and how the different elements of business models are related in order to generate revenues. This gap is addressed by another group of authors that strive to systematically work out components that are common to all business models and that can be used to better classify and analyze business models. Representatives of such ontological approaches are Osterwalder 2004; Amit & Zott 2001; Morris et al. 2005; Linder & Cantrell 2000; Margretta 2002; Osterwalder & Pigneur 2010; and Lindgren 2011.

Osterwalder (2004) and Osterwalder & Pigneur (2010) have developed a comprehensive ontology of business models that consists of nine key elements of which all business models are made up (Figure 1). These nine key components are (see Osterwalder & Pigneur 2010):

- Customer segments
    - Different groups of clients that exist
- Value propositions
    - The value that is actually sold to the customer segments
- Channels
    - Delivery to customers through
        - Communication channels
        - Distribution channels
        - Sales channels
- Customer relationships
    - Relationships established and maintained with each customer segment
- Revenue streams
    - Monetary results from value propositions that are successfully offered to customers
- Key resources
    - All assets required to offer and deliver the previously described elements
- Key activities
    - The activities performed in order to offer and deliver the previously described elements
- Key partnerships
    - Activities that may be outsourced
    - Resources that may be acquired outside the enterprise

- Cost structure
    - All business model elements together result in the cost structure

<table>
<tr><td rowspan="2">Key Partners</td><td>Key Activities</td><td rowspan="2">Value Propositions</td><td>Customer Relationships</td><td rowspan="2">Customer Segments</td></tr>
<tr><td>Key Resources</td><td>Channels</td></tr>
<tr><td colspan="2">Cost Structure</td><td colspan="3">Revenue Streams</td></tr>
</table>

Figure 1: Business Model Canvas of Osterwalder & Pigneur

Based on this approach, it is evident that our analysis of business models goes beyond what is predominantly described in the public debate as cloud computing business models. When cloud computing business models are mentioned, they are often only referring to the viewpoint of cloud computing platform / infrastructure providers. However, in order to capture the economic importance and value of cloud computing we have to acknowledge that there is a theoretically unlimited variety of value propositions, ranging from cloud platforms to all kinds of cloud services, that can form a cloud computing business model.

2.3 Business Model Risks

Like all business models, every cloud computing business model bears advantages and disadvantages. We define business model risks as any risk that has the potential to significantly affect a company's or business unit's ability to achieve the aims (primarily revenues) pursued by its business model.

In general, business model risks can be identified with tools like the Arthur Andersen Business model risk Model. According to this model, generic business model risks can be captured by the following (non-exhaustive) list of areas (Figure 2):

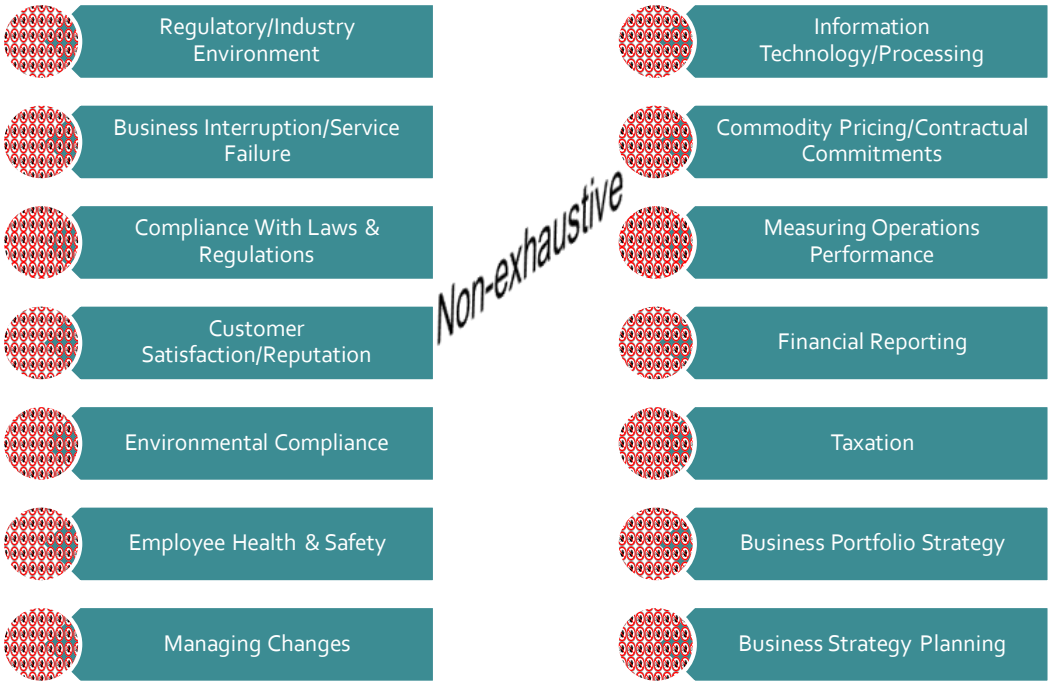

Figure 2: Business Model Risks (Arthur Andersen)

Examples of business model risks that may derive from cloud computing are

- Changes of the IT ecosystem that require adaptations of traditional IT business models (see the following chapter)
- Cloud effects on the customers' or partners' perception of a company and its products and services (e.g. when the company decided to migrate to cloud computing but does not see that partners or customers are reluctant to cloud computing)
- Unawareness of the management and skills capacities required to manage the cloud and the business processes in a cloud environment
- Unawareness of the costs of cloud computing, which may result in losses due to inappropriate pricing

Shi & Manning (2009) argue that business model risks can affect a business model in various ways at three different levels: The business model element level, the between-element relationship level, and the whole system level. The elementary risks relate to dangers and uncertainties for each of the components of a business model (Shi & Manning distinguish only four such components, but their approach is easily extendable to newer approaches with more key components), relationship risks are understood as compatibility risks that indicate potential misfit between business model components; and system risks are dangers and uncertainties that affect the business model as a whole.

The authors have developed a business model risk matrix (see Table 1) that distinguishes risks at the level of the value chain / value net, risks that affect the firm's share in the value of the market, and risks affecting the competitive sustainability of the firm.

	Value of Market	*Firm Share*	*Competitive Sustainability*
Elementary	**Decreasing customer value due to** • changing customer needs and wants • decreasing benefits of core offerings • decreasing value of complementary offerings • increasing competition in core offerings **Decreasing values for supplier, complementor or competitor due to** • increasing opportunity costs in the value net	**High operating costs due to** • inefficient organizational model • high costs of supplies **Weak profit regime due to** • lack of competitive core technologies • lack of control over complementors or suppliers • lack of competition among complementors or suppliers	**Deteriorating value of firm resources due to** • loss of rarity • competitive imitation

	Value of Market	*Firm Share*	*Competitive Sustainability*
		Weak positive cash flows due to • weak revenue streams • high operating costs • low returns on investments	
Compatibility	**Organizational failure in delivering a system that** • provides core offerings • attracts quality suppliers • attracts complementary offerings • maintains healthy competition to ensure customer values **Lack of adequate resources for organizational model to realize designed benefits, such as** • deficiency in key enabling resources and capabilities • inability to acquire, develop and keep key enabling resources and capabilities	**Failure of organizational model in** • balancing between delivering innovation and delivering efficiency **Failure of exchange model in** • keeping complementors and suppliers under control • keeping competition under control **Failure to resource model due to** • deficiency in key enabling resources and capabilities • inability to acquire, develop and keep key enabling resources and capabilities **Failure to make adequate investments in enabling resources and organizational systems**	**Incompatible exchange relations caused by increasing control of focal firm's resources by competitors, complementors, or suppliers** **Resources irrelevant to profit logic** **Firm resources are less effective in energizing the organizational model** **Changes in organizational models that are less capable of exploiting the full potential of the firm resources**

	Value of Market	*Firm Share*	*Competitive Sustainability*
System	**Decreasing customer value due to increasing competition from other value nets** (e.g., alternative technology platforms) **Collapse of value net induced by deteriorating value to certain economic actors**	**Merger or dissolution of value net causing a reduction of the focal firm's profit**	**Deteriorating resources based on which the entire value net thrives among alternatives**

Table 1: Business model risk matrix

From a business perspective, cloud computing becomes an option when it provides economic advantages and when the risks that come along with it can be mastered. There is no concept of 'trusted cloud computing' in business economics that resembles concepts and methods that exist in computer science and software engineering. Instead of such a concept, we argue that cloud computing provides a number of opportunities for the enhancement of existing business models and business processes and the development of new business models. These opportunities are endangered by a number of business model risks.

Therefore, we have developed an approach that generally distinguishes between

a) Cloud-related business opportunities (reflected in the motivations of firms to migrate to cloud computing)

b) Cloud-related business model risks

The risks, which are particularly important for requirements regarding reliability, resilience and trustworthiness, can be further distinguished as

a) Economic and organizational risks

b) Privacy and security risks

Overall, we have to deal with business model risks at four levels, which partly overlap:

- Generic business model risks
    - e.g. risks resulting from overall changes of markets or the ecosystem, which might result indirectly from the introduction and dissemination of cloud computing
- Cloud-specific business model risks
    - e.g. risks resulting directly from effects cloud computing effects on the business environment and business processes
- Economic and organizational business model risks
    - e.g. effects on costs, pricing, and business processes
- Privacy and security risks

- e.g. business model architectures or business relationships that subvert the security procedures and mechanisms set up on the cloud platform (i.e. through unawareness of security requirements from the cloud)
- these business model risks will provide primary input for the evaluation activities in Activity 3

The key purpose of this approach is to better explain how business aspects are affected by cloud infrastructures and how they impact requirements from cloud computing. This implies that the business model and business model risk assessment carried out in Activity 1 cannot limit itself to a pure technology assessment of the components developed in ACTIVITY 2. Overall, the business model and business model risk assessment of Activity 1 consists of three steps

1. Match the TClouds scenarios (home healthcare, public lighting) to the business model canvas
2. Identify business model risks and allocate them to the four levels (this will be carried out in interviews and a workshop, see section 2.4)
3. Match the four categories of business model risks to each element of the business model canvas

In a final step, the identified risks will be evaluated with regard to the level at which they can be addressed:

- Infrastructure / platform
- Management / organization
- Application / processes

With regard to the purposes of the specific evaluation of privacy, security and resilience issues of the TClouds platform and the usage scenarios in WP3.3, those risks that refer to these three aspects will feed in the subjects that will be tested and assessed in ACTIVITY 3.

2.4 Methodology for the Identification of Business Model Risks and Scenario Building

2.4.1 Principles and Objectives

According to Steyaert & Lisoir (2005, see also Schwartz 1991, van der Heijden 1991), scenarios can be conceptualized as narrative descriptions of potential futures that focus attention on relationships between events and decision points."

Scenario building exercises appear particularly useful when a multitude of factors exist that may affect the subject under scrutiny, i.e. when there is a high degree of uncertainty about the future. Such situations are, for instance, given when

- the problem is complex and multifaceted
- there is a high probability of significant change
- the dominant trends may not be favourable and thus must be analyzed
- the time-horizon is relatively long
- various factors exercise diverse and maybe contradictory effects on the subject

The basic purpose of scenario building is to identify driving forces, trajectories of development, key contingencies and key risks and challenges. The main objective of the TClouds scenario workshop is to generate alternative trajectories for future developments. In

addition, the documentation of the scenario results in form of a white paper may also provide the opportunity to lay out an experts' vision and action-plan for realisation.

2.4.2 Procedure and Stages

As Steyaert & Lisoir (2005) point out, the preparation for a scenario building exercise can vary extensively. The usual way to build scenarios is to set up a series of workshops where stakeholders discuss and identify the most relevant issues regarding the subject they have to evaluate. The scenario builders are free to use either a larger group or smaller teams, whereby the latter may be used to collect the input of others.

It is therefore no wonder that a scenario building exercise is expected to take approximately six months in total and including workshops of at least two full days and up to one week (5 days) (Steyaert & Lisoir 2005: 27). This variation is due to a number of topic-related factors, such as the complexity of the problem or the diversity of stakeholders involved, and methodological variables. Regarding the latter, a complete scenario building workshop that involves the same group of stakeholders in a collaborative process covering all stages of the scenario building, from the identification of key factors, driving forces and trends to the development of initial scenarios and their subsequent condensation into a small number of final scenarios, requires that the stakeholder group works together for a number of days. Alternatively, if the key factors, driving forces and trends can be identified by other means, the effort needed for the final scenario building can be significantly reduced.

Given the time and cost constraints that would be aligned with such an approach, it is obviously impossible to convince relevant business and academic experts to take part in a scenario building workshop that lasts 2-5 days. Therefore, the experts' involvement and efforts should be reduced to a minimum by combining scenario building methodologies with other methods, such as expert interviews and Delphi[1]-like expert consultations. The basic idea is to use expert interviews in order to collect insights in diverse stakeholders' views on cloud computing trends, challenges and drivers and to achieve a first validation of this information through iterative rounds of questionnaire-based evaluations by the expert panel that takes part in the whole process of scenario building (i.e. including interviews, Delphi evaluations and the final scenario building). The surveying of the experts through the research team will be done by email and possibly online via the TClouds website, where, for instance, short statements resulting from preceding expert interviews can be validated by means of Likert scales (Likert 1932) and with the purpose to cluster results in form of initial scenarios.

The Delphi method appears particularly useful for the purpose to identify relevant drivers, trends and challenges of cloud computing, as Linstone & Turoff (2002: 4) characterize following rationales as particularly suitable for the Delphi approach:

- "The problem does not lend itself to precise analytical techniques but cart benefit from subjective judgments on a collective basis
- The individuals needed to contribute to the examination of a broad or complex problem have no history of adequate communication and may represent diverse backgrounds with respect to experience or expertise
- More individuals are needed than can effectively interact in a face-to-face exchange
- Time and cost make frequent group meetings infeasible

[1] See Dalkey & Helmer-Hirschberg (1962), Linstone & Turoff (2002, first published 1975) and Steyaert & Lisoir (2005).

- The efficiency of face-to-face meetings can be increased by a supplemental group communication process
- Disagreements among individuals are so severe or politically unpalatable that the communication process must be refereed and/or anonymity assured
- The heterogeneity of the participants must be preserved to assure validity of the results, i.e., avoidance of domination by quantity or by strength of personality ("bandwagon effect")"

It should be noted that the last point in the list above usually results in the requirement to secure that the experts involved in the Delphi process remain anonymous. However, since we consider the Delphi approach only as an auxiliary measure to prepare the final scenario building, which, in contrast, requires direct interaction between these experts, this requirement has to be ignored for the purposes of the TClouds scenario workshop.

As a conclusion, the methodology of the TClouds scenario workshop consists of three steps:

1. Conducting interviews with experts from the two areas of the TClouds scenarios (home healthcare and public lighting) and from other relevant industries
2. Perpetual validation of interview results regarding key drivers, challenges and trends of cloud computing through short online and / or email questionnaires in order to build initial scenarios
3. Final scenario building at the TClouds workshop

2.4.2.1 Expert Interviews

There are two kinds of interviews that contribute to the scenario building process. The first group consists of interviews that helped to get an overview over key problems and directions of cloud computing and of the two application scenarios. We call these interviews, which were conducted at different points in time and with different methodologies during the first year of the project, pilot interviews. The other kind of interviews is carried out in the second year and aims directly at the scenario building and evaluation. We would like to call these interviews case study interviews.

2.4.2.1.1 Pilot Interviews

Overall there were 5 pilot interviews. The first one was conducted with Elmar Geese, an Identity and Access Management (IAM) expert and CEO of tarent AG, a German SME, in December 2010. This interview was designed to get an overview of the key factors that support or hinder the dissemination of cloud computing in European markets. The interview was an open interview centred around three questions:

- What are the experiences with customers when cloud computing is discussed as an offering?
- What are the driving factors of cloud computing?
- What are the key obstacles of cloud computing?

The results were that at the time of the interview cloud computing was a buzz word that many vendors and clients have used, but often without knowing exactly what it really means and what implications it has for IT infrastructures and business processes. The whole debate was geared by the seemingly enormous cost savings that could be achieved with cloud computing. Given the fuzziness of the term and prevalent privacy and security concerns, it was not possible to say whether cloud computing will become a key trend or slow down, like

it has happened to GRID computing before. A key recommendation received from this interview was to continuously monitoring the markets.

The other pilot interviews dealt with the two TClouds application scenarios in order to assess their position with regard to the state of the art and privacy and security issues from a business perspective. To this end, a group discussion was set up for the public lighting scenario. Experts involved in this group interview were from EDP (Miguel Areias plus some of his team members), EFACEC (Paulo Jorge Santos) and an external public lighting expert, Dr. Martin Beer from the Sheffield Hallam University. This group interview was organized along the scenario description provided by EDP and EFACEC and was evaluated from a business perspective. A key outcome of this group interview was that the original plan to outsource network management capacities to third parties, e.g. municipalities, would likely result in strong security and availability issues, as it is not probable that a third party from outside the energy supply industry would have the knowledge and capacities to manage a network properly. As a consequence, the scenario has been changed, EDP has decided to keep control over the network.

The same methodology was foreseen for the pilot interviews regarding the other TClouds application scenario (home health care), but due to last minute declines of some experts and scheduling problems of another expert these interviews have finally been carried out in a written form. The experts involved in these interviews were Professor Vicente Traver Salcedo from ITACA (Polytechnical University of Valencia) and Dr. Jos Aarts from the Institute of Health Policy and Management of the Erasmus University of Rotterdam. Key outcomes of these interviews were that the home health care scenario appeared as cutting edge, implying a number of challenges in mastering business processes between vendors and users in a secure way that protects especially the privacy of the patients. Nevertheless, both experts agreed that technically as well as from an organizational point of view the scenario was developed with a strong emphasis on limiting these risks. Both regarded user empowerment as the critical element for the success of such a scenario, whereby Dr. Aarts pointed out that user empowerment can only be implied on the technical level, while it must be generated and actuated at the level of the user himself. Thus, the end user and his capacities to oversee and understand what is going on in the cloud was considered to be the weak point in this scenario.

2.4.2.1.2 Case Study Interviews

In the case of the TClouds scenario building, the whole process starts with the expert interviews. Overall, the interviews aim to gain knowledge about the following aspects:

- critical trends, especially very long-term trends that are expected to continue
- factors of change or future-shaping events that could alter even trends that appear most established
- the roles of different stakeholders in the area
- events that can alter the environment in the future
- factors affecting privacy and security of cloud computing

The interviews will be carried out by phone and are designed in a way that allows the experts to answer the questions within 30-45 minutes. Areas and example topics will be structured as follows:

- *Generic information:*

  Cloud user / provider, Industry, Company size, Kind of cloud (public, private, hybrid, community), Kind of cloud services offered / used, Cloud provider (for users), Value propositions

- *Industry background*

  Role of cloud computing in industry, Driving forces in industry, Driving forces for company, Key trends in industry, Key challenges in industry, Key challenges for company, Goals, experience and strategy

  Goals: What are the key objectives / what is the basic motivation? What expectations are aligned with cloud computing? Where do these expectations come from (e.g. internal demand analysis, external consultancy, general cloud hype etc.)? What is the time frame?

  Familiarity / experiences with cloud computing and virtualization: When did the cloud computing project start / when is it intended to start? Is / has cloud expertise been available before the cloud project started? If not: How is / has this expertise been built up (training, external expertise, on the job)

  Cloud strategy: Who came up with the idea (department, consultant, partner, client)? Who is responsible? Is there an explicit strategy? How is it structured? How is it monitored and evaluated?

  Business strategy: Minimize costs, maximize value, mixed strategy

- *Technical aspects*

  Status / adaptation of cloud computing / software architecture: Is there anything on which the cloud can build upon? If to be developed: How is this capacity built up?

  Existing / planned IT environment and appropriateness for cloud computing, IT capacity analysis and management: Is there any analysis? What kind of analysis (technical considerations, commercial considerations, responsibilities, criteria)

- *Economic aspects*

  Cost analysis (degree / depth): Is there a cost analysis? Who carries out the cost analysis (department, internal or external)? What does the cost analysis involve (technical processes (data transfer etc.), organizational efforts, HR efforts, business model re-design)?

  Benefits: What savings are expected? What revenues are expected? Can savings / revenues be quantified?

  Partner network and key resources: In which way are business partners involved in or affected by the cloud project? Does the company rely on resources that were not necessary before the introduction of the cloud?

  Tasks: New tasks emerging from the cloud? How are new tasks handled?

  Customers: New customers through cloud? New offerings? Cloud impact on customer relations?

  Channels: Cloud impact on communication, distribution and sales channels?

- *Privacy and security*

  Measures to secure privacy and security: What are the reasons to believe that the cloud is secure (e.g. no critical data, secure technology / architecture (e.g. trusted computing), personnel (CSO and the like), governance (policies and guidelines), certification)

Risks and liability: What risks exist? For whom? Who would be liable? What is covered by SLA?

Cloud control and management: Who manages the cloud? How is it controlled? Cloud metrics, and commercial criteria. Perception of transparency? What can be done in cases of failure or frauds?

2.4.2.2 Delphi-like evaluation

The second step consists of a first rough evaluation of interview results through the stakeholders. The research team will analyze the interviews in order to retrieve information about

- Key motivations and driving forces of cloud computing
- Key trends
- Key challenges

Each of the items identified from the interviews shall be evaluated by measuring the experts' attitude towards the importance (or, in other words, the expected impact) of these items. To this end, the items will be made accessible on the TClouds website and a Likert scale will be used, like the one illustrated in Figure 3.

not important [1] [2] [3] [4] [5] very important

Figure 3: Likert scale for measuring attitudes

A second task the stakeholders should perform on the website is to indicate how certain or uncertain they are with regard to the role each of the items play. To this end, a similar Likert scale will be used.

Finally, the experts should determine which of the items they consider corresponding and which ones seem contradictory or unrelated to them.

The experts should have following questions (based on Ringland 2002) in mind in order to guide their assessment:

- Critical issues: Would you identify what you see as the critical issues for the future?
- A favourable outcome: If things went well, being optimistic but realistic, think about what you would see as a desirable outcome.
- An unfavourable outcome: As the converse, if things went wrong, what factors would you worry about?
- Lessons from past successes and failures: Looking back, what would you identify as the significant events that have produced the current situation?
- Decisions that have to be faced: Looking forward, what would you see as the priority actions that should be carried out soon?
- If you were responsible: If all constraints were removed and you could direct what is done, what more would you wish to include?

Based on this part of the evaluation the research team will identify a set of 5-10 initial scenarios that provide the key input for the final scenario workshop. These initial scenarios

may contain overlaps and a high degree of uncertainty, but they will be distinguishable by key driving forces and directions and their key challenges.

If possible (i.e. depending on the progress of the evaluation through stakeholders), a condensed version of this material will be distributed to the key note speakers, who may or may not use this matter as input for their speeches.

2.4.2.3 Final scenario building

According to Schwartz (1991), scenario building consists of following processes, in general:

1. identification of the focal issue or decision;
2. identification of the key forces and trends in the environment;
3. ranking the driving forces and trends by importance and uncertainty; selecting the scenario logics;
4. filling out the scenarios;
5. assessing the implications;
6. selecting the leading indicators and signposts for monitoring purposes

Given our mixed methods approach, some of these processes will have been carried out before the scenario workshop takes place. The first step is carried out by the TClouds project, which has defined cloud computing trends and the aligned privacy and security concerns as the focal issue. The second step will be performed by the expert interviews. The third step will be done by the experts in the Delphi phase. The fourth step is twofold, as it consists of the development of 5-10 initial, overlapping and maybe uncertain scenarios from the outcomes of the Delphi phase by the scenario building team. This part is also carried out before the workshop.

The second part of this step provides the key purpose of the scenario workshop: Eliminating overlaps and reducing uncertainty through further clustering and validating the initial scenarios until 2-3 scenarios remain that the majority of the stakeholders considers to be viable. After a brief presentation of the initial scenarios by the TClouds scenario building team, this clustering will be achieved by discussing and evaluating following questions:

- How likely appears each of the initial scenarios?
- How relevant appears each of the initial scenarios?
- Which (elements) of the initial scenarios appear related to another scenario?
- Based on combinations of (elements of) the initial scenarios: What would be a viable best case scenario (regarding privacy and security)?
- Based on combinations of (elements of) the initial scenarios: What would be a viable worst case scenario?
- Which positive and negative factors drive the two extreme cases?
- How would a viable scenario in between the two extreme scenarios look like?
- Which factors would drive the moderate scenario?
- Which factors appear less important or even irrelevant for the final scenarios?

Steps 5 and 6 of the scenario building should particularly aim at privacy and security issues. These aspects will be discussed at the workshop particularly with regard to policy advice, which shall be published in collaboration with the stakeholders.

However, it is also relevant to perform the final two steps within the TClouds consortium, as they are relevant with regard to the evaluation tasks of Activity 3 (WP3.3). Discussing these points by the technical partners of Activity 2 and the use case designers of Activity 3 would serve as a means to intensify the WP3.3 activities across the TClouds Activities.

Guiding questions for the assessment (step 5) are:

- What technological, economic, regulatory and organizational requirements must be met in order to achieve the level of privacy and security that is associated with the final scenarios?
- What privacy and security issues remain unresolved in the final scenarios?
- How important are these unresolved issues for future cloud computing / the future Internet?
- Are their realistic approaches to solve the unresolved privacy and security issues?

The sixth step aims at the identification of criteria that help to determine and monitor in which direction cloud computing develops. To this end, following questions should be answered:

- What are the key differences between the underlying trends of each final scenario?
- Which of these factors have a particular impact on privacy and security?
- Which policies would be suitable to achieve desirable levels of privacy and security in future cloud computing.

The whole process of final scenario building will be based on moderated discussions and tools to assess and evaluate scenarios and their components. The moderation will be carried out by the UMM team, which will also document the scenario building process. Tools that will be used in order to validate and assess scenarios and scenario components are stickers (for comments, statements), tags (e.g. different-coloured flags), and scorecards.

2.5 Target Groups and Selection Criteria

The scenario building should be performed by experts from three target groups: healthcare, energy supply / public lightings, and cloud computing in general. Thereby, the selection of candidates for interviews and participation in the online discussion and in the workshop should make sure that cloud providers as well as cloud users are covered. In addition, business and security and privacy experts from academia should round out the scenario building team in order to avoid that the scenarios are too much determined by industry specific drivers and challenges. This circle of experts has been identified in year 1 for the pilot interviews. Finally, the selection of candidates should cover as many EU Member States as possible in order to achieve a real European perspective.

In order to meet these criteria relevant associations of companies have been identified, which are

- for the home healthcare scenario:
  - the European Health Telematics Association
- for the public lighting scenario:
  - the Global Public lighting Federation (GSGF)
  - the European Distribution System Operators for electricity (EDSO)
- for cloud computing in general:
  - EuroCloud

The members of the first three organizations have been completely selected for contacting them, the list of more than 250 EuroCloud members (March 2012) was sorted by random numbers, so that this list can be called until the threshold of 50 interviews has been achieved.

Thus, it should be noted that the list of candidates, which is attached in Annex 1, does not imply that we will interview all these entities, as this would exceed the capacities of the research team. The selection process secures that the final selection is indeed a random selection, and the interviews will stop when the 50th interview has been conducted. All members in the list in Annex 1 will however be invited to participate in the Delphi evaluation.

Chapter 3

General Trends in Cloud Computing

Chapter Authors:

Ruediger Glott (UMM), Kirsten Haaland (UMM), Andreas Meiszner (UMM)

Cloud computing, although widespread, is still in its infancy, as two thirds of the respondents of the Future of Cloud Computing Survey (North Bridge Venture Partners 2011) reported that they either are only experimenting with it (40%) or have plans to migrate to cloud computing but wait for the market to mature (see also Jefferey & Neidecker-Lutz (no date). The overall picture of cloud computing presented by experts is dominated by positive expectations of new business opportunities and, often mentioned as the most important cloud computing drivers, cost reductions, increased scalability and growing agility (e.g. Babcock 2010, Buyya et al. 2008, Hinchcliffe 2009). On the other side of the spectrum of opinions about cloud computing are experts that fear technological lock-ins or consider cloud computing as a marketing strategy to sell old solutions and services with a new package (Stallmann 2008, Greenemeier 2011).

Such views have also been reported in the pilot interview with Elmar Geese, CEO of tarent AG, a German SME. He pointed out that most companies seem to have a vague understanding of the opportunities and an equally vague understanding of the risks of cloud computing, while detailed knowledge to assess different technological and strategic options are usually lacking at the side of many (potential) cloud users. With regard to privacy and security Mr. Geese considered clearly defined, understandable, transparent and dynamic (adaptable) processes as the most important requirement. It should be clear at each stage of the processes within the cloud where keys are stored, who is responsible for what process, and what will happen in case of errors (e.g. outages) or fraud.

In recent years the question which of the cloud computing service models – IaaS, PaaS or SaaS – and deployment models – private, public, private or community cloud – (Mell & Grance 2011) – will become mainstream (e.g. Urquhart 2009) played a significant role in the debate about development trends of cloud computing. Meanwhile it appears that there is a clear trend towards public clouds for IaaS and SaaS, although the diverse field of 'other services' plays also a significant role, indicating that special purpose clouds may have a comparably large market share, too (see Figure 4). The 2011 Cloud Computing Outlook Survey (North Bridge Venture Partners 2011) confirms the trend towards the public cloud (used by half of the respondents, whereas private clouds are used by 24%).

[2] See The Guardian, September 28, 2008: Cloud computing is a trap, warns GNU founder Richard Stallman. Available online at: http://www.guardian.co.uk/technology/2008/sep/29/cloud.computing.-richard.stallman

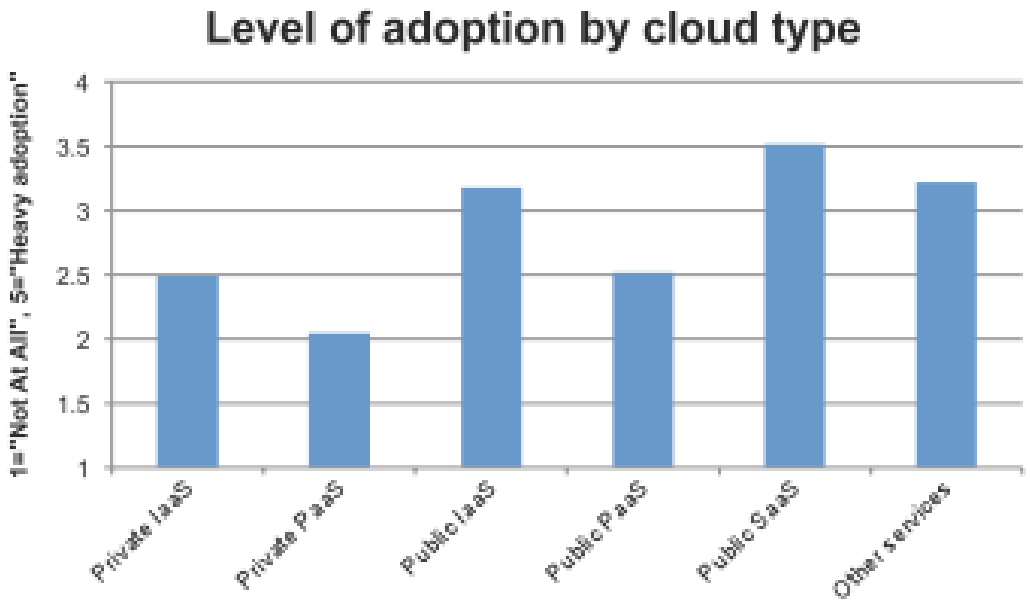

Figure 4: Adoption of cloud computing service and deployment models

Source: BITCURRENT 2011

Regarding the "market shares" of cloud providers (i.e. their respective share in the 130 survey respondents) there is some dynamics, e.g. a growing share of Microsoft Azure public cloud, but still Amazon Web S1ervices dominates the market, followed with some distance by Google App Engine (see Figure 5).

Though cloud protagonists repeatedly report about companies using clouds for business critical applications (e.g. BITKOM 2011[3], EMC 2010), survey data does not confirm a trend in this direction. Only 2% of the respondents of the 2011 Cloud Computing Outlook (North Bridge Venture Partners 2011) claimed that they use cloud computing for such applications (see Figure 6).

A closer look at cloud vendors' primary source of revenues indicates that SaaS subscription fees play the dominant role in the market, as 28% of the respondents of the 2011 Cloud Computing Outlook (North Bridge Venture Partners 2011) have stated (followed by fees for 'other services'; all other options are around or below 10%).

Finally, the expectation regarding the development of cloud computing revenues for the next few years are quite positive (see Figure 7).

[3] See http://cloud-practice.de/

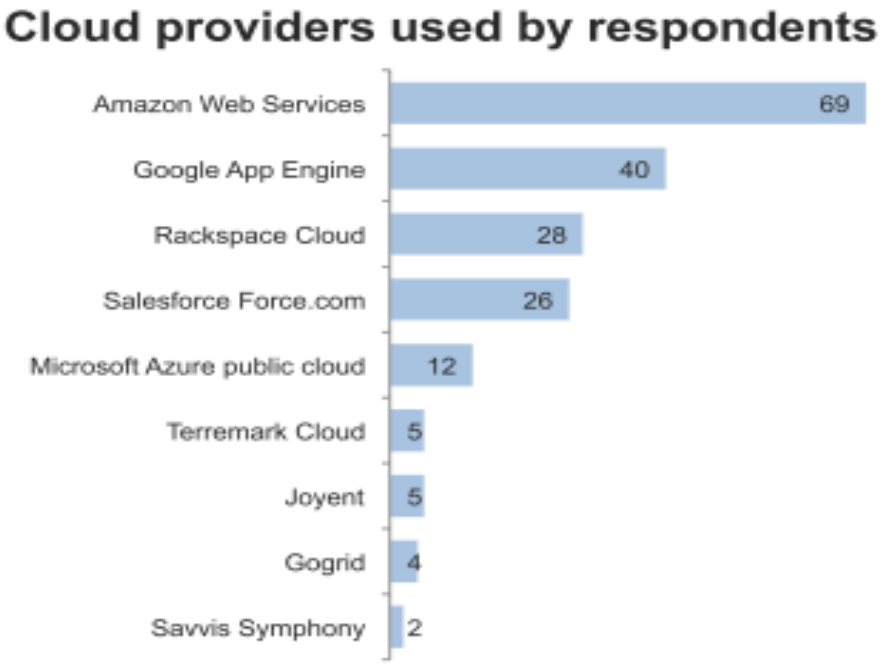

Figure 5: Cloud providers' market shares (survey respondents)

Source: BITCURRENT 2011

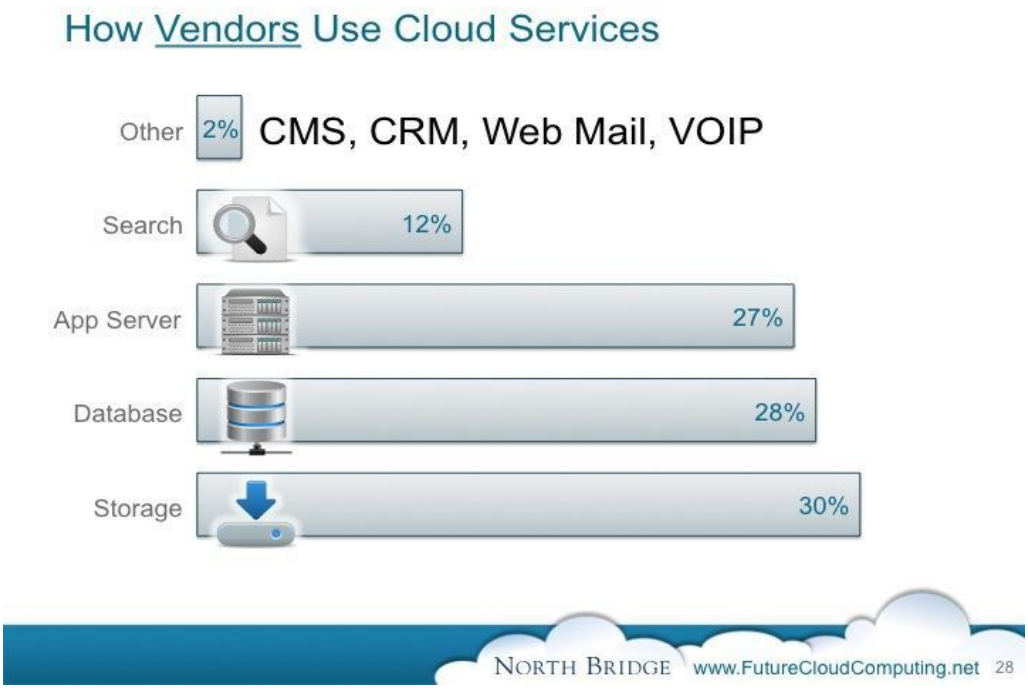

Figure 6: Purposes of cloud usage

Source: North Bridge Venture Partners 2011

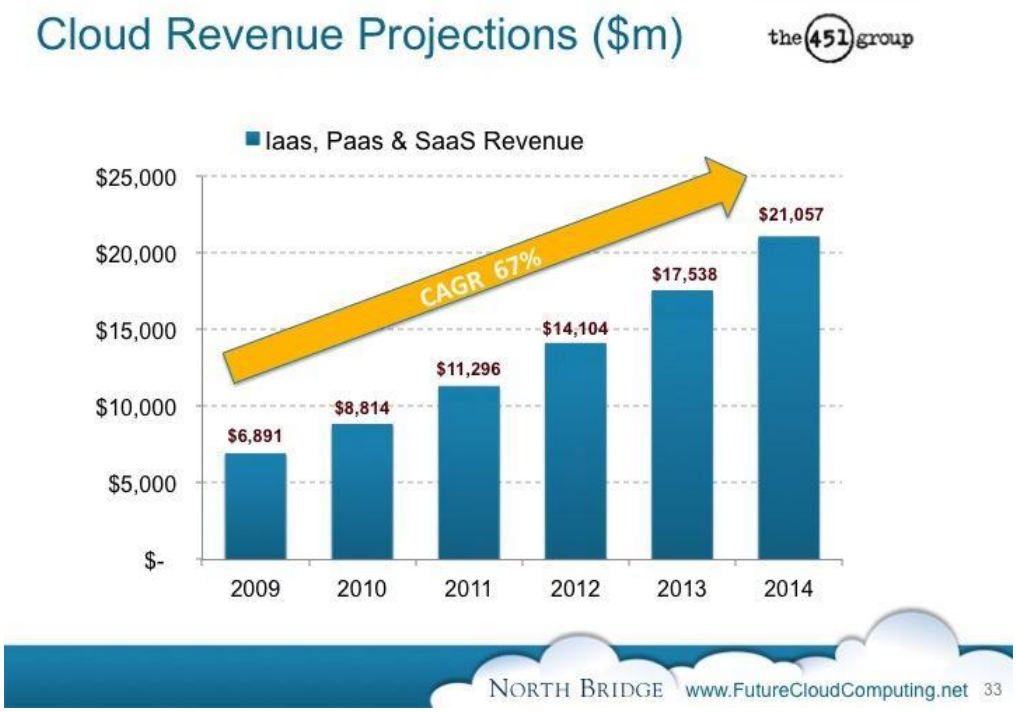

Figure 7: Cloud computing revenue trends

Source: North Bridge Venture Partners 2011

Finally, cloud computing has shown already some impact on traditional business ecosystems[4] in the IT sector (Standridge et al. 2011). It is expected that opportunities and challenges will hit different actors differently (ibid.). However, Standridge et al. (ibid.) believe that "the industry's entire value chain, including software vendors, hardware original equipment manufacturers (OEMs), service providers, distributors, resellers, and retailers—will operate very differently from the way it has in the past." In particular, the traditional tight relationships between fundamental groups along the value chain, such as independent software vendors (ISVs); OEMs; systems integrators (SIs), distributors, large-account resellers (LARs), value-added resellers (VARs); and retailers will probably weaken. Through the growing independence of software sales from physical channels the complexity of the value chain and the relation between its actors is expected to decrease (ibid.).

In particular, Standridge et al. (2011) expects the role of traditional IT delivery players (software distributors, resellers and e-sellers, VARs, and LARs) to decline. In addition, it is likely that the value of customization and integration will decline, which would affect especially the SME market. Finally, certain delivery and selling assets will likely increase in value. Players that are capable to combine direct sales relationships, subscription billing

[4] Moore (1996: 26) characterizes business ecosystems as "an economic community supported by a foundation of interacting organizations and individuals—the organisms of the business world. The economic community produces goods and services of value to customers, who are themselves members of the ecosystem. The member organisms also include suppliers, lead producers, competitors, and other stakeholders." In a later extension (or clarification) of this definition, Moore (1998: 168) explains that a business ecosystem is an "extended system of mutually supportive organizations; communities of customers, suppliers, lead producers, and other stakeholders, financing, trade associations, standard bodies, labor unions, governmental and quasigovernmental institutions, and other interested parties. These communities come together in a partially intentional, highly self-organizing, and even somewhat accidental manner."

relationships, e-commerce storefronts, hosted infrastructure, and secure application delivery will benefit from the changes induced by cloud computing. It therefore appears that service providers, including telecom operators, cable companies, and hosters, are potentially well positioned in the emerging cloud market, especially with regard to consumer and SME markets.

Overall, Standridge et al. (2011) considers four factors to be decisive for the further adoption of clouds and the reconfiguration of the cloud ecosystem:

1. The level of customization and integration required to provide enterprises with the cloud-based software they need
2. The extent to which security, privacy, and auditability issues are resolved in public clouds, and across different verticals
3. The degree to which consumers – as employees – succeed in actively shaping demand for business applications and related tools and devices
4. The extent to which new aggregation opportunities open up at the application (SaaS) and platform (PaaS) levels, and the speed with which players move to capture these new opportunities — becoming, in effect, the new distributors for the cloud-based technology ecosystem

In the following three sections we will present a summary of the two TClouds application scenarios and the TClouds platform together with the privacy, security and resilience requirements and characteristics they feature. It must be noted that detailed use cases and privacy, security and resilience requirements are provided in the respective deliverables of ACTIVITY 2 and ACTIVITY 3, to which we refer in the following sections. However, we will not provide all these details here but limit the discussion to examples from these deliverables in order to illustrate where and how the design of the platform or of the services and processes at the application level (i.e. the scenarios) bear potential business model risks. A detailed mapping of application scenario elements and business model risks is currently under work for WP3.3.

In the concluding chapter, we will evaluate where the scenarios stand with regard to the overall trends that we have observed, the feedback from the expert talks, and the business perspective on risks aligned with the platform and the scenarios.

Chapter 4

TClouds Home Healthcare Scenario

Chapter Authors:

Mina Deng (PHI), Milan Petković (PHI), Marco Nalin (HSR), Ilaria Baroni (HSR), Imad Abbadi (UOXF), Eva Schlehahn (ULD), Ruediger Glott (UMM), Kirsten Haaland (UMM

4.1 Health Trusted PaaS

Health Trusted PaaS (Health TPaaS) is at the core of TClouds. This is a summary of Health TPaaS, a more extensive description can be found in section 5 of D3.1.2, as well as (Deng at al., 2012). As the name indicates, Health TPaaS' focus is on functionalities and services available at the Platform as a Service (PaaS) layer. Further, it is important to note that some of the services interface towards end users, and hence in effect fall under the Software as a Service (SaaS) level. Overall, the Health TPaaS is a multi-level platform aiming to:

- Store trustworthily health data in compliance with privacy regulations
- Enable third party application on the platform by providing APIs that allow the access to users' data, as well as the ability of third parties to use the available identity and role management services
- Allow the end users to manage their own data and determine which application and provider can access which data
- Provide log services and auditing mechanisms for authorization requests, user's data access, apps and data management and policy administration

From this high level description of TPaaS services, it is clear that the Health TPaaS interfaces towards actors at various levels. There are two main categories of actors, namely the end user (including both the professional end user and the common user), and administrators (platform administrator, application administrator - including the application developer and the application manager). (The various actors are defined in D3.1.2 section 2.2.2). Hence Health TPaaS interfaces towards users being actual end users, and towards developers of third parties applications. It also interfaces towards applications deployed on the platform itself, as well as underlying infrastructure layers.

Though Health TPaaS strives for security and resilience at the technical level and tries to make the corresponding requirements transparent to the users, from a business perspective it is obvious that this environment where the actors engage raises various business model risk issues. Users are required to adapt their non-technical relations (through business models and business processes) in accordance with the privacy and security principles that guided the design of the TPaaS.

4.2 Actors

Actors in the home healthcare scenario are:

- General Practitioner
- Patient
- Medical professional (e.g. Psychiatrist @ Hospital)
- Health and Wellness Service Provider (e.g. Activity monitoring service)
- Pharmacy
- Family
- Region/national infrastructure (e.g. an authority such as the Department of Public Health)

4.3 Use Cases

The use cases may be grouped into five functional packages, namely user management, relations/privacy management, auditing, application management, and monitoring and benchmarking. The use cases can be split into end users' activities, application administrators' activities, and platform administrators' activities.

End users' activities includes (but is not limited to): new user registration, user self-deletion from the system, user self-deletion of single data, user deletes single data of another user, social relationships definition, addition of new relation between user and application and data access auditing. The application administrators' activities includes (but not limited to): provider registration, application registration (and applications' privacy and policy specifications), modification of application signature, application deletion, application manager request of access logs, and new user registration. Platform administrators' activities includes platform auditing at both the PaaS level and IaaS level, as well as the checking of load balancing and performance monitoring.

Taking a closer look the application administrators' use case UC 130 concerning the modification of app signature (new app version):

Use case unique ID	**UC 130 – Modification of app signature (new app version)**
Description	A third party's developer has added new functionalities to the app and needs to extend/modify the minimum policy requirements of the app
Actors	Developer, users of the app
PreConditions	The third party's developer is registered and logged into the system and the app is already registered
PostConditions	The new app profile is registered into the system with the new related privacy policies
Normal Flow	1) The third party's developer goes to a specific page within her personal area in which she can see all her app registered in the system and she selects the app of which she wants to modify the privacy policy. 2) The system asks the new App signature info (version, new privacy policies, …) 3) The responsible confirms the changes.

Use case unique ID	UC 130 – Modification of app signature (new app version)
	4) The system will send a notification to the app's users (those users that already have a relation with the app) and asks them to accept the new privacy policies User can either ○ accept the new policies ○ deny the new policy and maintain the old privileges (this might lead to app malfunctioning, but it will be responsibility of the app providers to solve the issue)

Use case unique ID	UC 140 – App deletion
Description	A third party's developer wants to delete permanently her app to the platform
Actors	Third party developer, users of the app
PreConditions	The third party's developer is registered and logged into the system and the app is already registered
PostConditions	The app is not registered anymore
Normal Flow	1) The developer goes on a specific page in the restricted area on the platform website to remove apps 2) She selects the app she wants to remove and confirms it 3) The system will send a notification message to all the app's user with the reminder that within a certain period of time (e.g., 30 days) the application will be permanently deleted from the platform 4) After a given time period (e.g., 30 days), the system: a. Will remove automatically the app signature and the app will no longer be able to use the TPaaS API. b. Will remove the relation between the users and the app

4.4 The Business Model Perspective

As laid out in the section on the home healthcare scenario, the value proposition of this scenario is treatments in order to prevent or cure depressions. The key partners are

Traditional Healthcare Service Provider

- Hospitals (as key providers of the treatments)
- Healthcare professionals

Institutional Service Providers

- Pharmacies
- National/Regional Authorities (e.g. Department of Public Health)
- Delivery Service Operators

Health and Wellness Service Provider

- Health and Wellness Service Providers (e.g. Activity monitoring service)

The customers are the patient/user, and possibly the family.

The critical elements of the business model with regard to the business model risk assessment are the key activities that form the overall interplay between the key actors and the customer relationships and channels (see section 4.6). These elements depend highly on the capacities and constraints of the underlying cloud of clouds and on the capacity of the involved cloud users to notice and react to malfunctions and errors (see chapter 6).

Finally, the cost structure and the revenues will also depend to some degree on the ways and means the cloud of clouds provides to secure key activities of the partners and protect the privacy of the customers. In this context, next to technical and organizational aspects legal issues and compliance play a significant role.

While it is possible to offer the services this scenario aims at in return for subscription fees, which would be in line with the current overall trend in cloud computing, it could also be an option to offer basic services for a general subscription fee and premium services for additional fees. Such a pricing model would resemble the pricing models in many national healthcare systems.

4.5 Technical Security and Privacy Requirements

The following provides an overview over cloud-specific security and privacy requirements from the home health-care scenario.

Business driven requirements of the healthcare use case

Generic cloud-specific requirements	
Self-managed services	Cloud computing should facilitate automated self-managed services to support clouds' virtual resources availability, reliability, resilience, scalability, security and privacy, and adaptability.
Highly distributed data storage	Data are not stored at local data stores, but data stores are highly distributed in the cloud.
Requirements for healthcare in the cloud	
Semi-trusted (or honest but curious, passive) model	Semi-honest model is assumed that the cloud providers (including cloud employees and system administrators) are semi-trustworthy (or honest but curious).
Data-centric protection	• Electronic health record (EHR) data have to be protected in a highly distributed way by different systems with complex and maybe legacy architectures, even if some of which may not have a trustworthy data management system. • The center of the protection is at data stores/centers.
Emergency access and availability	It is important to guarantee the timely availability of medical data, especially under emergency cases. This in term requires the availability of the decryption key if data are encrypted at data stores.
Efficiency	Access control mechanism must be sufficiently efficient to be leveraged in the processes of medical care. Given the short time doctors currently have to spend with patients, it is unacceptable if the system performance is too slow to satisfy business needs.
Data confidentiality	• Fine-grained access control is required to provide confidentiality of data. • Unlike multimedia or entertainment data, even partial leakage of patients' medical data is undesirable. • The access control policy should not only be role-based, but highly context-based (or rule-based). For instance, patients may have a trust relationship with their current medics, while disregard the relationship with their former medics. • The access control and key management mechanism should be secure and efficient. Private / secret keys should be securely stored and protected. • Data can be potentially accessed by a variable set of parties from different domains with different rights. There is a large uncertainty in who will eventually need to access a data object. It is thus implausible to implement central management. • Potential side channel leakage of medical data should be prevented. (For example, the fact that someone takes an HIV test demonstrates that he/she is considered at risk.) It is a desirable to define rules that protect side channel information without disrupting normal healthcare.

Data integrity	• The integrity of medical data should be guaranteed to facilitate the correct medical care for patients. • The integrity of logging / auditing data should be guaranteed to ensure system accountability / auditability.
Accountability	Data access and usage or certain operations in the system have to be logged. In many cases, the context allowing data access cannot be determined automatically, but only verified by a human after the incident. In this regard, auditing is desired with some automated verification procedures.
Patient-centric protection	• Access control: Patients should be able to specify/delegate the access control rights / policies of their medical data. • Usage control: Patient should be able to control how their data is used and to which party it is distributed. • Patients should be aware of their privacy rights (i.e. refer to legal requirements).
Data minimization & anonymization / filtering	• According to the European Data Protection Directive 95/46/EC (EU, 1996), the principle of data minimization means that "a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfill that purpose. In other words, data controllers should collect only the personal data they really need, and should keep it only for as long as they need it". • Data needs to be anonymized or filtered (i.e. to remove personal identifying information) under certain scenarios, e.g. for clinical research or studies that require data secondary use. Or it is according to patient's privacy preferences, e.g. when PHR is shared with healthcare institutions, it may be necessary to remove part of the data before sharing with healthcare institutions.

4.6 Business Model Risks

In this section we refer largely to the scenario description of D3.1.2, which contains a detailed overview of use cases, actors, and security requirements and elements. We will not reproduce all these detail in this section but focus on a few illustrative examples in order to highlight how technical and application (services, processes) design may impact the underlying business model. A detailed and complete mapping of business model risks to the security and privacy features of the two scenarios is currently under preparation for WP3.3.

All the use cases relating to the end users' activities and the fact that the user is empowered and can enable/inhibit others actors from accessing their data, assumes that the user is able to understand and implement these changes. It is not clear that all end users have the skills to monitor and audit who, how and when their data is being accessed, or take the correct actions and manage their own privacy settings.

Further, relating to use case UC 130 where the third party developer requires a new authorization where a third party's developer has added new functionalities to the app and needs to extend/modify the minimum policy requirements of the app. After the system has sent a notification to the end users, the user can accept or reject the new policies. If the new policy is rejected, this might lead to application malfunctioning, where it is the responsibility of the application providers to solve the issue and it is not an issue with the platform itself per-se, but it is a real business model risk.

Relating to the benchmark application from Health TPaaS concerning the personal advice application, in general, the upload of data can only be performed by a doctor, and allows the

patient to manage her data and be redistributed to other Service Providers. There is a potential problem with identity management, because even if technically only a doctor has access, it is well known from other healthcare processes that the doctor who should be the only one with access or authority, may distribute these tasks to other individuals (including username/password). In other words, technically the actors may be well defined, but it does not necessarily follow that these are the same actors in reality. On an organizational level, as well as on a business level between actors, other communication channels exist and the control mechanisms can be subverted.

Similarly, knowing the security rules and mechanisms in place, may lead to circumventing these mechanisms and that data may flow through other channels and partnerships that exists, even if there is technically not possible to have a data or information flow on the cloud.

Another business model risk is the actual migration to the cloud, the porting and development costs forms an important barrier. As the development and migration costs decrease, and the potential availability of data and other third party suppliers increase, the value to a given service provider increases. There must be a return on investment for third parties to be interested in porting to the platform.

The dynamic service composition enabled by Health TPaaS is a benefit for the application Service Providers, as it allows a more dynamic service composition and marketing strategy. It follows that it is easier for a provider to change the commercial partner. On the one hand this is an advantage, reduces lock-in to a specific application or commercial partner. However, on the other hand, a Service Provider that currently is in a dominant position in the market with a large market share and enjoying the benefits of the lock-in and dependency on their technology, might see it as a risk to enter into a situation where effectively they potentially give up market power and subject themselves to increased competition. From an overall welfare perspective it is clearly better that provider can change commercial partner more easily, but for a third party considering migrating and the associated costs, the benefits must outweigh the costs.

One business model risk that may occur in the home healthcare scenario may derive from the decision to install the Trusted Platform as a Service (TPaaS) on Sirrix Infrastructure based in Germany (see D3.1.2). While this decision might make sense from the viewpoint of the service vendors within the home healthcare scenario because they know Sirrix and its technology and trust in both, the patients that operate at the periphery of the cloud and third parties that do not belong to the key partners within the cloud infrastructure might not feel well about the fact that data about their person / company or their clients is stored outside their national jurisdiction. While the effect appears negligible for a pilot, the real life implementation of such a scenario should only be considered after careful market research in order to assess the acceptance of a business model that involves foreign partners.

Another source of business model risks may derive from the way how actors and their relations are defined on the platform (see D3.1.2). The basic idea is to allow actors only those rights that make sure that they cannot harm users' security and privacy or the cloud's resilience. For instance, application developers and application managers are assumed to be unable to have relations with users, professionals or apps. However, given that in the healthcare system actors will not only interact via the channels (distribution, sales and communication) provided by the cloud but that there will be use of other channels (telephone, face-to-face, through IT systems outside the cloud), too, it appears impossible to avoid that personal information (about users or clients) will be built up and stored in quantities and places that are not foreseen by the cloud. In this case, the cloud should be able to at least prevent the owners of these unintended data to distribute it within the cloud. From a business model perspective, this implies that the channels of the business model must be clearly defined and controllable.

Regarding the cost structure and the pricing models that were discussed in section 4.4, the crucial question is whether privacy and security may be offered at different levels, so that a basic level of privacy and security is provided with the general subscription fee, while higher levels of privacy and security would cost the client (a service provider or the patient) extra money. Such a model would largely correspond to the models applied by providers of privacy and security services, such as antivirus software vendors.

This decision can probably not be made ex ante and for all involved parties because the cloud strategy, which includes certain decisions regarding privacy and security, has to be aligned with the capacities of the involved parties and the overall business strategies of these partners. If the cloud strategy is very strict, in this regard, service vendors that might add value to the overall services provided through the cloud may not be able or willing to use this platform, or they would be forced to offer their services at prices that do not return sufficient revenues.

These aspects played also a role in the expert interviews with Professor Vicente Traver Salcedo from ITACA (Polytechnical University of Valencia) and Dr. Jos Aarts from the Institute of Health Policy and Management of the Erasmus University of Rotterdam. They both confirmed that the technical and architectural design of the home healthcare scenario is state of the art or even ahead of state of the art. However, while Professor Traver Salcedo highlighted particularly the attempt of the scenario to protect the patient and to empower him as a user of the system, Dr. Aarts cautioned that the user's power is not just a function of the technology but also bound to her own skills and capacities.

It should be noted that this ambiguity seems to apply to both prototype applications suggested in D3.1.2. The Philips-Respironics Actiwatch is a benchmark application where the data upload could be done only by a doctor but also the patient is assumed to be able to manage her data and to ensure its trusted redistribution to other services providers, if needed. The other benchmark application, the Wellbeing Portal allows the depressed patients to self-manage their disease in collaboration with a number of different service providers in order to collect and analyze data, including the possibility to show the trends of sleep Activity, light exposure and mood variations. The patient can authorize her doctor (e.g., her psychiatrist) to watch her data, and the application allows to the patient to specify privacy policies to limit the information that should be displayed to the doctor. To add data in her personal records, the patient has two possible ways: the system can reuse data uploaded from other Service Providers properly registered, authenticated and authorized (e.g., the personal device application described above), or the patient can insert manually data in the system, through the Wellbeing Portal application. As a conclusion, a well-defined and well-functioning business model that operates on the cloud platform may be harmed through unaware end users, so that despite the high level of security the platform and the application design and management provides the platform may get a bad reputation. In this regard, transparency, control facilities and ease of use for the end user seem to be crucial prerequisites to make efficient use of the platform's high level of security and resilience.

Regarding the home healthcare scenario, one medical expert pointed out that the use case that was chosen for the application scenario (depression treatment at home) has very specific implications on how the cloud system works. He assumed that a less delicate use case might have been better applicable and testable. On the other hand the expert also understood that depression is a disease that particularly calls for treatments that can be applied at home, as patients with this disease might be lethargic and not willing to leave their home. At any rate, it was recommended to take the specifics of the use case into account when the cloud system shall be transferred to another use case.

Chapter 5

TClouds Public Lighting Scenario

Chapter Authors:

Miguel Areias (EDP), Miguel Grossinho (EDP), Paulo Viegas (EFA), Paulo Santos (EFA), Alberto Rodrigues (EFA), Ruediger Glott (UMM), Andreas Meiszner (UMM)

5.1 Introduction

A Public lighting transforms the way power is distributed and used, adding intelligence throughout the grid to dramatically reduce outages and faults, improving responsiveness, handling current and future demand, increasing efficiency and management costs. The Public lighting uses sensor meters, digital controls and analytic tools to automate and monitor the flow and delivery of energy to consumers, enabling a two-way flow of electricity and information among the power plant, the appliance and the points in between. Through Public lightings it is also possible to incorporate new sustainable energies such as wind and solar generation, and interact locally with distributed power sources, or plug-in electrical vehicles.

As part of a Public lighting, the Smart Lighting System will provide public lighting management functionalities like on/off commands, real time status, energy consumption and schedules update. The accuracy and timely information in those systems is crucial because decisions are taken in real time. No information, or information later in time, represents inaccurate analysis that will turn in bad decisions. To prevent this kind of situations, information must be suitably protected. This is especially important in the increasingly interconnected world.

Information security for Public lighting infrastructure feeds from information security enforced on the electric sector world and the telecommunications world. Both these worlds have systems which deal with millions of customers, highly critical assets for the functioning of society, storing sensible customer information, and potentially generating detailed information about customer habits.

In particular the Smart Lighting System, as a system designed for control the public lighting, does not have critical data related with customers consumptions, making data confidentiality as part of the information security issues, less critical than data integrity, availability or authenticity.

5.2 System Architecture

The Smart Lighting solution will be a web application that will let authorized users to interact with the underlying Public lighting infrastructure in order to operate and/or extract information from the public lighting sub-system, thus enabling a more efficient management over the public lighting service. Therefore, the solution must include a set of management capabilities like on/off commands, real time status, energy consumption and schedules update.

The overall solution consists of several components which, articulated among themselves, allow us to address the objectives recognized for the system. The main components of this solution are:

- **IT Systems:** systems and applications for management and central data processing such as energy metering management and commercial systems.
- **SCADA/DMS (Supervisory Control and Data Acquisition/Distribution Management System):** Systems and applications for supervision, control, optimization and management of power distribution networks.
- **Distribution Transformer Controller (DTC):** local control equipment to be installed at switching stations (including modules for measuring, actuation, processing, interface, communication, etc.).
- **Energy Box (EB):** devices to be installed at consumers/producers (including modules for measuring, actuation, processing, interface, communication, etc.).

Figure 8 depicts the overall system architecture.

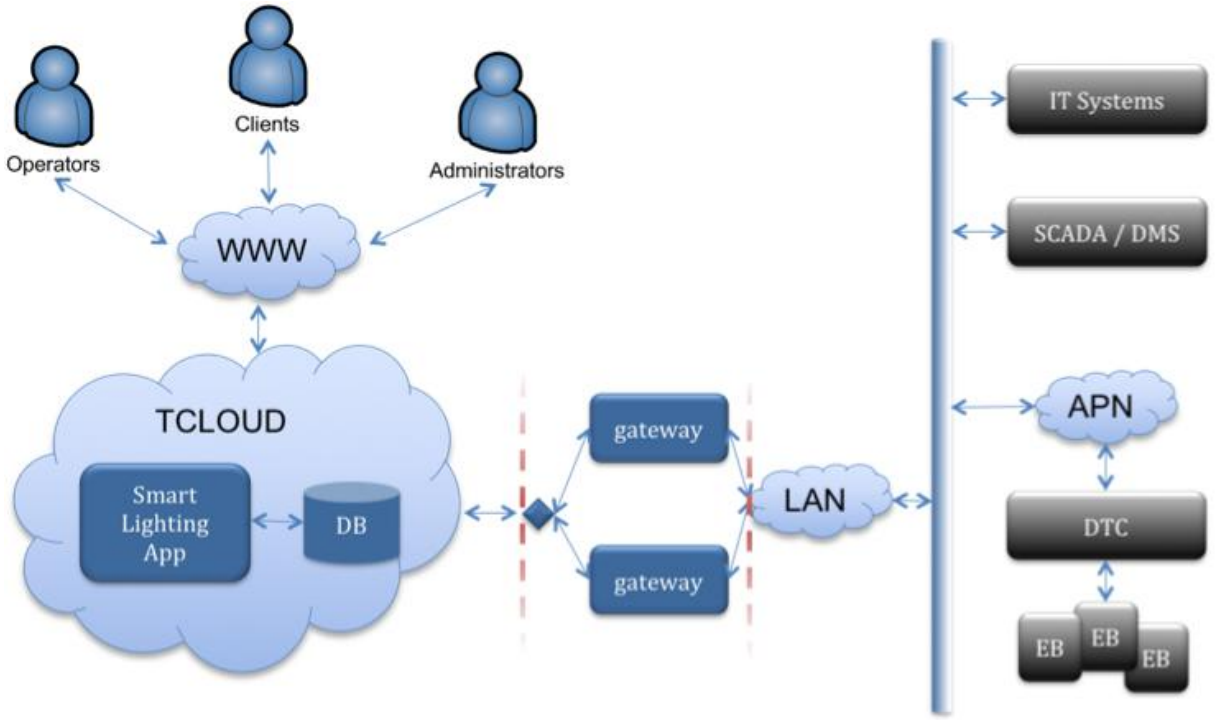

Figure 8: Smart Lighting Architecture

5.3 Actors

The following actors were identified:

- Operators (Municipalities, EDP)
- Clients (Municipalities)
- Administrators (EDP)

5.4 Business Functions

At a high level, the Smart Lighting solution must provide the following business functions:

- Monitor consumptions
- Monitor state and anomaly events (alarms)
- Manage lighting services and schedules
- Manage public lighting settings
- Actuate over control circuits
- Manage settings of public lighting intelligent devices (DTC & EB)

5.5 Use Cases

In this section we collect the use cases that help on understanding the business functions that were identified for the Smart Lighting System. We organize the use cases into four main categories:

- Public Lighting Management
- System Administration
- Alarm Management
- Reporting

Figure 9 depicts the four use case categories in the form of high level use cases.

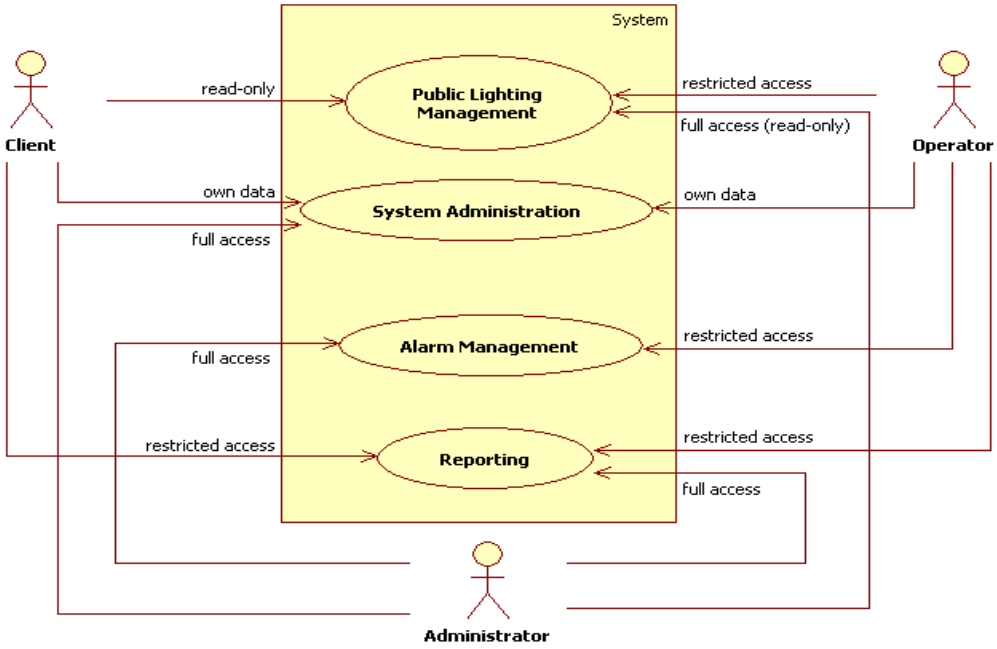

Figure 9: Smart Lighting High Level Use Cases

Throughout these use case diagrams, the following access rights applies:

- Own data: read-write access to the user's (e..g. a municipality) personal data.
- Read-only: read access to whole data.
- Restricted access: read-write access to data belonging to the user Operational Area.
- Restricted access (read-only): read access to data belonging to the user Operational Area.
- Full access: read-write access to whole data.
- Full access (read-only): read access to data belonging to the user's Operational Area (see below).

The Public Lighting Management set of functions lets users operate the Smart Lighting System, as is the case of Operators, or display information about the configurations that were applied to the system, if the user accessing the application is either a Client or an Administrator. The difference between the Client and the Administrator capabilities on this matter lies on the fact that the Client is bound to a so called "Operational Area", which is a concept used to define a subset of the network being operated, whereas the Administrator has read-only access to the whole available data.

The System Administration set of functions is used to access and manipulate user information. Both the Client and the Operator are only allowed to act on the information pertaining to them, whereas the Administrator has full access to all of the functions contained in this category.

The Alarm Management category deals with the ability both Operators and Administrators have to see abnormal condition events that are displayed in the form of alarms.

The last category that was identified for the Smart Lighting solution is the Reporting category, which enables users to generate reports about many of the operational aspects of the

system. Again, both the Client and the Operator have restricted access to these functions, since they are only allowed to see the part of the information that is relevant to the section of the system they are assigned to. As for the Administrator, there is no limitation whatsoever on the information he can access when using these functions.

5.6 The Business Model Perspective

The value proposition of the public lighting scenario is the provision of public lighting. Key partners are the network operators (EDP or municipalities), and the administrator (EDP).

Customers are municipalities.

The key activities include various monitoring and management services.

The key resource is the public lighting that has to provide capacities for performing the key activities and (a part of) the communication, distribution and sales channels.

Like in the other scenario, the ways and means the public lighting employs to meet these demands will strongly affect the cost structure and revenues that can be achieved. As mentioned for the case of the home healthcare scenario, organizational and legal (compliance) aspects will determine the interplay of actors and the technical architecture of the public lighting, which will affect the cost structure and revenues in the end.

5.7 Public Lighting Management

The Public Lighting Management category is the cornerstone of the solution in the sense that it contains most of the functions that let users operate the system. As the operation of a Smart Lighting System requires the configuration of several different aspects of the application, the resulting functions are quite numerous and hard to lay out on a single use case diagram (Figure 10).

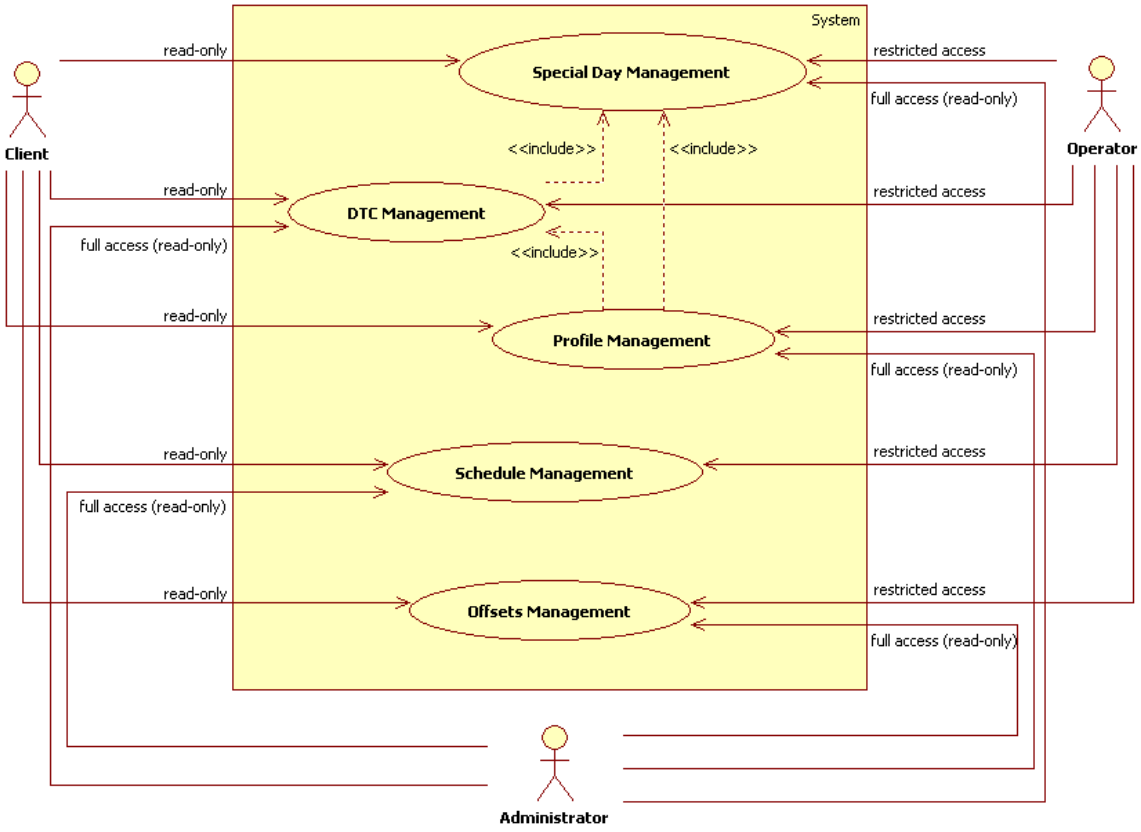

Figure 10: Public Lighting Management Diagram

The main purpose of Public Lighting Management use case is to manage DTC settings regarding the public lighting control. Therefore the Smart Lighting solution has to effectively map the relevant DTC data structures, in order to end users intuitively and efficiently manage public lighting settings.

5.8 Business model risks

Due to confidentiality reasons this scenario cannot be described and examined at the same level of detail as the home healthcare scenario. Nevertheless, one business model risk appears evident.

A key problem that turned out in the group interview with an, Dr. Martin Beer from the Sheffield Hallam University, and representatives from EDP and EFACEC is that the role of the administrator in the interplay of actors must be clearly defined, especially with regard to its relation to the operator of the grid. The reason is that, in contrast to the home healthcare scenario, where privacy protection and security concerns are the most relevant issues, the public lighting relies very much on resilience and security in order to secure availability of the service. Therefore, operator knowledge appears as an indispensible precondition to secure the availability of the service, which implies that the administrator should not have the right to modify grid settings.

As a consequence, this scenario is less open and involves fewer actors than a scenario like the home healthcare scenario. Therefore, control over and access to the grid remains centralized.

Chapter 6

The TClouds Platform Architecture

Chapter Authors:

Imad M. Abadi (OXFD), Ilaria Baroni (HSR), Johannes Behl (FAU), Alysson Bessani (FFCUL), Sören Bleikertz (IBM), Sven Bugiel (TUDA), Christian Cachin (IBM), Emanuele Cesena (POL), Miguel Correia (FFCUL), Mina Deng (PHI), Ruediger Glott (UMM), Thomas Groß (IBM), Michael Gröne (SRX), Kirsten Haaland (UMM), Andreas Meiszner (UMM), Marco Nalin (HSR), Stefan Nürnberger (TUDA), Michael Osborne (IBM), Marcelo Pasin (FFCUL), Gianluca Ramunno (POL), Paulo Jorge Santos (EFA), Roberto Sassu (POL), Norbert Schirmer (SRX), Matthias Schunter (IBM), Paolo Smiraglia (POL), Klaus Stengel (FAU), Davide Vernizzi (POL)

The TClouds approach to a cloud of clouds concept can be reasoned as follows (Deng et al., 2012):

"TClouds is built upon a set of principles: (1) Flexible trust models: cloud consumers shall be able to determine their individual security and privacy preferences to provision user-centric protection. (2) Federated ecosystem of independent cloud providers: it prevents cloud services depending on any individual provider. Benefits include reduced cloud lock-in and switching cost, simplified migration and standardized APIs, and to avoid monopolistic structures. (3) Scalable security mechanisms: the security architecture does not break the underlying cloud principles, and is scalable, transparent, and resilient against failures of the underlying virtual infrastructure. (4) EU legislation compliance:

From a business perspective, it is obvious that particularly the 2nd point is relevant. However, as we have seen in the discussion of the business risks aligned with the cloud computing application scenarios, the first point is relevant with regard to the risks at the level of the cloud user, and the third point is relevant with regard to securing the desired degree of transparency. The fourth point, i.e. legal considerations, plays a role for each business by nature.

From a business perspective, increased privacy, resilience and security are highly valued because they improve the quality of the value propositions and probably help to increase the acceptance of cloud computing. Therefore, any component of the cloud platform architecture that contributes to enhancing these features of the cloud should appear as meaningful from a business perspective. In this sense, technical criteria like confidentiality, integrity and availability are equally important on the level of business models and business processes.

Activity 2 of the TClouds project has identified 15 components that are intended to ensure privacy, security and resilience of the TClouds cloud of clouds. Table 2 illustrates what these components do and if they play a role in the usage scenarios.

Component	Type (Paas/IaaS)	Confi-dentiality	Integrity	Availability/ Dependability	Medical	Grid
CheapBFT	Cloud-of-Clouds (PaaS)		Masking of errors	Resilience against provider attacks		✓
Simple key / value store	Cloud-of-Clouds (PaaS)	Encryption of Storage		Minimized trusted computing base	✓	✓
Secure Block Storage	Trusted Cloud (IaaS), Open Stack	Encryption of Storage	Access with integrity proofs		✓	✓
Secure VM Instances	Trusted Cloud (IaaS), Open Stack	VM access restricted	Boot-time integrity check		✓	✓
Trusted Server	Trusted Cloud (IaaS), Sirrix	Secure virtualization and isolation	Boot-time integrity check		✓	✓
Log Service	IaaS / PaaS	Confidential logging	Write-only logging	Availability of logs despite attacks	✓	✓
State machine replication	Cloud-of-Clouds (PaaS): state machines		Masking of errors	✓		✓
Fault-tolerant workflows	Cloud-of-Clouds (PaaS): business processes		Masking of errors	✓	✓	✓
Resilient object store	Cloud-of-Clouds (PaaS)		Object checksums	✓		✓
Confidentiality proxy for S3	Cloud-of-Clouds (PaaS) with IaaS key management	Object encryption			✓	
Access	Cloud-of-	Enterprise			✓	

Component	Type (Paas/IaaS)	Confi-dentiality	Integrity	Availability/ Dependability	Medical	Grid
control as a service	Clouds (PaaS)	rights management				
Trusted objects manager	Trusted Cloud (IaaS), Sirrix	Object encryption, security policy management	Object checksums, remote attestation		✓	✓
Trusted management channel	Trusted Cloud (IaaS), Sirrix	Confidentiality of management	Accountability of management		✓	✓
Ontology-based reasoner	IaaS / PaaS	Detection of unauthorized access	Detection of configuration integrity issues	Validation of dependable configurations	✓	✓
Automated validation of isolation	Trusted Cloud (IaaS), Open Stack	Detection of isolation breaches	Detection of potential attacks		✓	✓

Table 2: TClouds privacy and security components matrix

Overall, the 15 TClouds components selected by ACTIVITY 2 are[5]:

- *CheapBFT*
  - CheapBFT will be designed in order to ensure availability, reliability and integrity of services hosted in a trusted cloud even in the presence of arbitrary faults.
- *Simple key/value store*
  - Simple key/value store is an example for a simple cloud service component that can be used by other services to cache non-critical data, i.e. dynamically generated frontend websites; it secures that the service and stored data are safe from unintended modifications.
- *Secure block storage (SBS)*
  - Block storage is non-linear raw memory attached to VM instances as block device (virtual hard disk, e.g. iSCSI). SBS will provide a transparent layer that provides security properties such as confidentiality, integrity and authenticity for block devices. The SBS is also responsible for user-centric key management. For TClouds two types are relevant: 1. Public Clouds: The infrastructure of public clouds cannot be changed. Hence, the security properties must be provided by means established inside the VM. This can for example be achieved by encrypting the block device, e.g. encryption of Amazon's EBS2 using TrueCrypt in EC2 instances. 2. TClouds – OpenStack: As the infrastructure can be modified, transparent security properties can be

[5] The brief descriptions of the components are taken from D2.4.1.

added to e.g. the hypervisor in order to provide legacy VM with confidential, integrity-protected and authentic block storage.

- *Secure VM Instances*
    - Is a component that allows clients to securely deploy, launch, and migrate their own VM images. The component ensures that the VM images and data contained within will be confidentiality and integrity protected when they are at rest in a image repository or in transit during migration. The authenticity can be ensured using a secure channel.
- *Trusted server*
    - SRX will provide the TrustedServer as the central security platform to run the VM instances (also called compartments). It provides isolation of compartments by linking them to TVDs. Domain specific transparent encryption is applied to prohibit information flow between TVDs. The focus of this component is to provide (together with TrustedObjects Manger (TOM) a trusted platform for cloud applications from the ground up.
- *Log Service*
    - Log Service is the TClouds logging subsystem, mainly used by other Cloud Components to log their internal events and, possibly, by applications. Log Service can be used as basis for auditing or reporting the Service Level Agreement (SLA) compliance to the User (here the main target of the service is the end user of the cloud, but it may also refer to an external auditor or to the Cloud Admin).
- *State machine replication*
    - Any secure system can be deceived by exploiting its known defects, so measures that allow for tolerating intrusions must also be addressed when building the trustworthy clouds. To cope with this problem FFCUL is providing a state machine replication library that ensures integrity and availability of replicated services as long as at most a fraction of the replicas (usually less than a third) are compromised.
- *Fault-tolerant work-flow execution*
    - Fault-tolerant work-flow execution is a PaaS infrastructure permitting the fault-tolerant execution of business processes in particular and workflows in general which are based on and composed of Web services. The infrastructure will be based on BPEL2, an XML-based language for describing such workflows.
- *Resilient object storage*
    - The object model for cloud storage has become extremely popular, after its introduction with Amazon's Simple Storage Service (S3) in 2006. It allows reads and writes of simple blobs, each one identified by a unique name (also called a "key"). A multitude of commercial providers offer such blob storage services today. We will contribute a system that builds reliable and secure storage through a federation of object storage services from multiple providers. Multiple clients may concurrently access the same remote storage provider and operate on the same objects. They do this through an interface that contains the basic and most common operations of object cloud storage. (Since every vendor provides the same basic operations but slightly different advanced operations, the system only uses the common denominator of all providers.)

- *Confidentiality proxy for S3*
    - Integrating untrusted Amazon Simple Storage Service (Amazon S3 [amab])-based storage into the trusted cloud infrastructure is another approach to reach resilient storage. Therefore the trusted cloud infrastructure needs a middleware component. SRX will contribute to the trusted cloud infrastructure with a confidentiality proxy for S3. The component is implemented as a security service which is part of the security kernel and managed by TOM. It will transparently encrypt data of a mounted file system (Linux) according to a TVD and allows to integrate untrusted S3-based storage into the trusted cloud infrastructure.
- *Access control as a service*
    - Provides automated management of clouds virtual resources.. Such automated management would require understanding the properties of cloud infrastructure and its policies, and it would also require understanding cloud user requirements. Cloud user requirements should be continually considered by cloud provider by matching user requirements and infrastructure properties in normal operations as well as during incidents. We are planning to develop an Enterprise Rights Management (ERM) tool, which we refer to as Access Control as a Service (ACaaS).
- *Trusted objects manager (TOM)*
    - The Trusted Objects Manager (TOM) is the central management component of the trusted cloud infrastructure. The TOM manages the physical infrastructure including networks, services and appliances (physical platforms). Since appliances remotely enforce a subset of the overall security policy, a permanent trusted channel between the TOM and its appliances is used for client authentication, to check their software configuration using attestation, and to upload policy changes and software updates. Finally, for each Trusted Virtual Domain (TVD) defined the TOM creates an independent TVD-specific Root-CA. SRX will contribute by enhancing the TOM to manage the Trusted-Servers within the cloud infrastructure.
- *Trusted Management Channel*
    - The Trusted Management Channel allows to securely connect the TOM with TrustedServers to set-up, start and stop VM instances, and to load configuration and policies. It also could be used to interconnect TOMs. The Trusted Management Channel is part of the overall security concept of of Trusted Infrastructures.
- *Ontology-based reasoner to check TVD isolation*
    - The ontology-based Reasoner is a subcomponent/plugin for the Management Component that, given as input a service model, an infrastructure model and an allocation of services onto the infrastructure, makes it possible to verify whether some security properties required by the service are satisfied by the allocation. Furthermore, it may also provide hints on how to modify the allocation whenever security requirements are not met.
- *Automated validation of isolation of cloud users*
    - SAVE (Security Assurance for Virtual Environment) is a tool developed at IBM research for extracting configuration data from multiple virtualization environments, transforming the data into a normalized graph representation, and subsequent analysis of its security properties. IBM will integrate and

adapt this technology for the demonstrator based on OpenStack, in order to validate isolation of cloud users.

It would be optimal if each of these 15 elements, or a composite of some of them, would correspond to an equally clearly defined business model risk. However, the technical components are targeting, at a fine-grained level, at very specific security and resilience functionalities, for which no corresponding requirements or functionalities exist at the level of business processes and business models.

Therefore, a one-to-one or one-to many matrix describing the relation between these components and business requirements from cloud computing does not exist. The reason for this is that business requirements are rather aggregate, aiming at privacy and security in general (and usually combining these demands with other goals like cost-efficiency or user-friendliness), while the technological components address specific functions that help to achieve these aggregate features.

This implies that a) not all technical components relate to an equally fine-grained business model risk or opportunity and b) not all business requirements and risks can be addressed on the level of the components of the technical platform, i.e. it is likely that there are business requirements beyond the cloud platform (e.g. related to applications or business processes that can be performed on this infrastructure). Nevertheless, there are significant business model risks that can be related to an architectural component or to the composite of all the components together. On this background, it appears useful to consider these 15 TClouds components at a more aggregate level. Overall, these 15 elements can be aggregated in three groups:

- Trusted infrastructure
  - Secure block storage
  - Secure VM instances
  - Trusted server
- Trusted management
  - Trusted Objects Manager
  - Trusted Management Channel
- Platform services (trusted cloud of cloud services)
  - Cheap BFT
  - Simple key / value store
  - Log service
  - State machine replication
  - Fault-tolerant work-flow execution
  - Resilient object storage
  - Confidentiality proxy for S3
  - Access control as a service
  - Ontology-based reasoner to check TVD isolation
  - Automated validation of isolation of cloud users

At this aggregate level, it appears that trusted infrastructure and trusted management largely correspond to business model risks such as business interruption and information

technology/processing, trusted management to measuring operations performance, and platform services to service failure and measuring operations performance.

However, given this rather weak correspondence between the technical security elements and business model components or particular business model risks, the key problem seems to lie in aligning these technical components and their role for the cloud strategy with regard to privacy, security and resilience on the one hand and the overall business strategy of the cloud users on the other hand.

For instance, it is possible that a cloud strategy that strives to provide a maximum of security and privacy contradicts the overall objectives that a company strives to achieve with its general business strategies. For example, a maximum security strategy for the cloud might result in overburdening a company with costs, skills requirements and organizational complexity.

Another issue, from the business perspective, is that it might be unclear what criteria can be applied in order to determine which of these components should be implemented and used. For instance, the home healthcare scenario plans to employ only eight out of these 15 components, based on the analysis of technical needs in order to perform all the processes planned in this scenario in a secure and resilient way. However, it is not evident whether – and to what degree – the considerations of the ACTIVITY 3 team that have led to this decision are applicable to other business scenarios. The role of the 15 components for the resilience of the public lighting public lighting has not been published yet.

In general, from a business point of view each of these components as well as the composite effects of all the components together must be considered with regard to following questions:

- How familiar and experienced has a cloud user (client or administrator) to be in order to benefit from this element?
- To what degree has an existing cloud computing / software architecture to be adapted in order to use this element efficiently?
    - These questions relate to cost and skills issues that an organization that wants to tap the potential of this element has to master Familiarity / experiences with cloud
    - With regard to the business model, necessary skills can either be provided in-house or through an external partner that has the capacities to master a cloud with this element.
    - This might imply that cost advantages that are gained from this element on the technical level and that improve the quality of the value proposition (through increased resilience, privacy and security can be partly or fully consumed by organizational (staff composition, composition of key partners) changes and search cost related to these changes. In this case, the technical advantage would not unfold the intended effect, and cloud users might abstain from this opportunity for the same reason – high costs – that causes the current reluctance towards implementing BFT elements in cloud platforms.
- How does the element fit into the customer's cloud strategy and goals?
    - This question relates to the key resources of the business model (technology) and their impact on the overall business strategy and the revenues the customer strives to achieve.
    - If a minimum cost strategy underlies the business model, a cloud strategy that strives for maximum security might be counterproductive in economic regards. This aspect must particularly be considered with regard to the 15 elements in total.

  - From a business point of view, it would be useful if each element can be determined with regard to implementation and operation requirements and costs.
  - Responsibilities and roles for the cloud implementation (department, IT vs. business) must be clarified and the goals of both strategies (cloud strategy and business strategy) should be aligned and made explicit. In this context, the specific impact of the elements on both strategies should be evaluated.

- What processes must be performed with the element to ensure privacy, resilience and security?
  - This question relates again to key activities and skills and has thus the same implications as described under the first bullet point.
- What is the impact of the element on cloud service offerings to users (clients, partners) with regard to control, transparency and the management of the cloud?
  - In general, we assume that each of the elements enhances resilience, privacy and security of the value propositions, so that the quality of the service offerings increases.
  - However, though each particular element might have this desired effect, the composite effect of all the elements together might be increased complexity and a loss of understandability, which might result in a loss of control.

Chapter 7

Conclusions

7.1 Overall Conclusions

The two application scenarios are intentionally very different, not only with regard to the sector (healthcare versus energy supply) but also with regard to the scope of actors and transactions to be performed within the respective cloud system.[6] The home healthcare scenario must be considered far more complex than the public lighting scenario. It must be noted that this observation does not imply any valuation; it is only neutrally referring to a phenomenological difference resulting from the intentional design of the responsible partners.

Nevertheless, with regard to the overall trends depicted in chapter 1 the two scenarios have a number of things in common, and there are also a number of things that distinguishes them. First of all, both application scenarios are not affected by the trend towards public IaaS or SaaS clouds because TClouds aims at the development of a cloud of clouds, which is not included in the NIST definition of cloud computing and either not asked for in surveys.

Since both application scenarios are open to or even foresee collaboration with commodity clouds it might be an advantage that their shares in the market grow, as this might imply that actors addressed in the scenario are already used to these clouds. Familiarity with commodity clouds may lower the entrance barrier to join the cloud systems designed by TClouds.

A significant difference between the two application scenarios exists with regard to the overall reluctance towards running business critical operations on the cloud. The public lighting scenario is built on the assumption that the grid cannot be totally open and must, in the end, be controlled by EDP because EDP is the only actor within the scenario who has enough knowledge about the grid in order to avoid outings or load imbalances. Hence, the public lighting follows the overall cloud trajectory, in this regard. The requirement of final control through EDP was a direct result of the expert talk, until which it was at least implicitly assumed that a sub-contractor of either a municipality or of EDP would be able to make critical decisions on the grid.

The home healthcare scenario, in contrast, depends on actors', especially the patients', willingness to release personalized data and to process critical operations on the cloud. In order to achieve this readiness, the involved partners have developed a trust model for their cloud system that enables the patient to impose access and deny rules on other actors when her data is requested. However, the expert interviews we have carried out revealed that it is not clear from the use case description how the patient can enforce her rules. In other words: The experts acknowledged that the home healthcare scenario aims explicitly at user empowerment, which is considered as a crucial precondition for the cloud system to operate as planned, but were unsure as to whether the user's will can be exercised to the demanded degree.

[6] For an explanation of the term 'cloud system', we refer to D1.3.1.

A positive factor for both application scenarios is the still positive revenue trend associated with cloud computing, as this might work as an incentive to actors targeted in the scenarios to join the cloud system.

All experts confirmed that the two application scenarios appear secure from the technical point of view. Due to the specific challenges the home healthcare scenario has to master, this scenario was considered as 'cutting edge', while the public lighting scenario was acknowledged for its strict 'safety first' decisions, which made it rather a state of the art cloud system. Thus, it appears that there is something like a vicious circle in cloud computing when personal data and business critical operations come into play, which is a higher demand for sophisticated security and privacy protection, which in turn is apparently raising concerns regarding security and privacy because these methods are, by nature, not as established and well tested as state of the art methods.

The approach to distinguish types of business model risks and to allocate these to the building blocks of the business model in which the cloud shall be implemented allows a holistic business model risk analysis that combines technical, economic and organizational aspects. However, there is no strong correspondence between fine-grained technological components to increase cloud security and business requirements. Business requirements are comparably aggregate, but to be met the interplay of a number of technological components is necessary. Nevertheless, it appears most important to find ways that allow an alignment of the cloud strategy, which includes decisions about the level of security and privacy protection, with the overall business strategy and the business model a cloud user operates. It seems that limited clouds with centralized control can be managed relatively easily and low cost, which can be covered by subscription fees. However, more complex cloud business scenarios that are open to a multitude of partners that can offer and combine their services on the cloud seem to require more diversified pricing models, and they feature high demands from the organizational and technical capacities and the skills of the involved parties.

Finally; related to the latter point, from a business point of view it appears necessary that the technology of clouds becomes more transparent and easier to understand and control in order to ease their usage and to be better able to calculate costs that are directly and indirectly aligned with cloud computing. Otherwise an approach like TClouds, which aims at high security and adaptability, may be countered by cost concerns.

7.2 Recommendations

Businesses that want to use the TClouds cloud of clouds need to know what requirements they have to meet and how expensive the implementation of TClouds security and resilience functionalities is. Therefore, we recommend that the project provides information about

- Cloud computing risks and how the TClouds cloud of clouds addresses these risks (i.e. general information about the functioning and its capacities)
- Technological requirements
    - the minimum requirements from the company's own IT infrastructure
    - the required level of familiarity with cloud computing
    - how the company can monitor whether the cloud works with the required degree of security and resilience, and how it can react in case of problems
    - the criteria to decide what security components / what level of security and resilience should be chosen
- Organizational requirements

    - what can be done by a company without IT department (e.g. sales store) and at what point is an ICT department or a partner that monitors and manages the cloud is recommended
- Skills requirements
    - what technical, legal and management skills are required
    - how these requirements change with varying degrees of security and resilience
- reference implementations (fictitious or actual), e.g. based on the experiences gained from the two TClouds scenarios in home healthcare and public lighting

Based on such information, each TClouds user would better be able to decide if and how business processes and business models are affected by the cloud and how they can be adapted to master the challenges aligned with cloud computing. Such adaptations can be, for instance, changes in staff or a strategic partnership with a cloud service / management provider.

Chapter 8

Bibliography

Al-Debei, M. M., and Avison, D., 2010. Developing a unified framework of the business model concept. European Journal of Information Systems, 19(3), 359-376.

Amit, R. & Zott, C., 2001. Value creation in e-business. In: Strategic Management Journal, Vol. 22, No. 6-7, pp. 493-521.

Babcock, C., 2010. Management strategies for the cloud revolution. New York et al.: McGraw Hill.

BITCURRENT, 2011. Cloud computing survey 2011. Available online at: http://www.bouledecristal.crim.ca/ressources2011/documents/Bitcurrent-Cloud-survey-2011-BC_BCCS_0311.pdf

BITKOM, 2009. Cloud Computing – Evolution in der Technik, Revolution im Business. BITKOM-Leitfaden. Available online at: http://www.bitkom.org/files/documents/BITKOM-Leitfaden-CloudComputing_Web.pdf

Buyya, R., Chee, S. Y., Venugopal, S., 2008. Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. Available online at: http://arxiv.org/ftp/arxiv/papers/0808/0808.3558.pdf

Casadesus-Masanell, R., Ricart, J. E., 2010. From strategy to business models and onto tactics. Long Range Planning, 43, 195-215.

Chesbrough, H. & Rosenbloom, R. S., 2002. The role of the business model in capturing value from innovation: evidence from Xerox Corporation's technology spin-off companies. Industrial and Corporate Change, Volume 11, No. 3, pp. 529-555.

Chesbrough, H., 2006. Open business models: How to thrive in the new innovation landscape. Boston, MA: Harvard Business School Press.

Chesbrough, H., 2010. Business model innovation: opportunities and barriers. Long Range Planning, 43, 354-363.

Cloud.com, 2011. 2011 cloud computing outlook. Survey results. Available online at: http://www.cloud.com/cloud-computing-outlook/survey.pdf

Deng, M. Nalin, M,, Petkovic, M., Baroni, I., Abitabile, M. and Sanna, A., 2012, Towards Trustworthy Health Platform Cloud, in IEEE CLOUD 2012 (submitted).

EMC, 2010. Die Virtualisierung geschäftskritischer Anwendungen. Technologiekonzepte und geschäftliche Überlegungen. Available online at: http://germany.emc.com/collateral/software/white-papers/h6859-virtzng-business-crtcl-appts-wp.pdf

Greenemeier, L., 2011. From Dot.Coms to Cloud Computing: What's Old Is New Again. Available online at: http://www.scientificamerican.com/article.cfm?id=dot-com-cloud-computing

Hinchcliffe, D., 2009. Eight ways that cloud computing will change business. Available online at: http://www.zdnet.com/blog/hinchcliffe/eight-ways-that-cloud-computing-will-change-business/488

Horsti, A., 2007. Essays on electronic business models and their evaluation. Helsinki: Helsinki School of Economics. Available online at: http://hsepubl.lib.hse.fi/pdf/diss/Activity 296.pdf

Jefferey, K. & Neidecker-Lutz, B. (eds.), no date. The future of cloud computing. Opportunities for European cloud computing beyond 2010. Expert group report. Brussels: European Commission. Available online at: http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

Linder, J C., and Cantrell, S., 2000. Changing business models: surveying the landscape. Accenture Institute for Strategic Change.

Lindgren, P. (ed.), 2011. Baseline for Networked Innovation Models. Available online at: http://neffics.eu/wp-content/uploads/2011/10/NEFFICS_D4.1_v1.0.pdf #

Margretta, J., 2002. Why Business Models Matter. Harvard Business Review, 80 (5), 86-92.

Mell, P. & Grance, T., 2011. The NIST Definition of Cloud Computing (Draft). U.S. Department of Commerce. Available online at: http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

Moore, J.F., 1996. The Death of Competition: Leadership & Strategy in the Age of Business Ecosystems. New York: Harper Business.

Moore, J.F., 1998. The Rise of a New Corporate Form. In: Washington Quarterly. Vol. 21(1), pp. 167-181.

Morris, M., Schindehutte, M., Allen, J., 2005. The entrepreneur's business model: Toward a unified perspective. Journal of Business Research, 58 (6), 726-735.

North Bridge Venture Partners, 2011. Future of cloud computing survey. Available online at: http://futureofcloudcomputing.drupalgardens.com/media-gallery/detail/91/436

Osterwalder, A., 2004. The Business Model Ontology, A Propositional in a design science approach. Universite de Lausanne, Ecole des Hautes Etudes Commerciales. Available online at: http://www.hec.unil.ch/aosterwa/PhD

Osterwalder, A., Pigneur, Y., 2010. Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers, Wiley.

Osterwalder, A., Pigneur, Y., Tucci, C. L., 2005. Clarifying business models: origins, present, and future of the concept. Communications of the Association for Information Systems, 16, 1-25.

Rappa, M., 2004. Business Models on the Web. Available online at: http://www.startupjunkies.org/business_models.pdf

Schlachter, E., 1995. Generating revenues from websites. In: Board Watch, July 1995. Available online at: http://boardwatch.internet.com/mag/95/jul/bwm39.html.

Shi, Y., Manning, T., 2009. Understanding business model and business model risks. Available online at: http://www.iae.univ-lille1.fr/SitesProjets/bmcommunity/Research/Shi_and_Manning_-2009.pdf

Standridge, D., Minasian, P., Seelbach, F. & Reich, J., 2011. Seeing Through the Clouds. Navigating the Evolving Technology Ecosystem. Booz & Company. Available online at: http://www.booz.com/media/uploads/BoozCo-Navigating-Evolving-Technology-Ecosystem.pdf

Teece, D. J., 2010. Business models, business strategy and innovation. Long Range Planning, 43, 172-194.

Timmers, P., 1998. Business models for electronic commerce. In: Electronic Markets, Vol.8, No. 2, pp. 3-8.

Urquhart, J., 2009. The three routes to cloud computing's future. Available online at: http://news.cnet.com/8301-19413_3-10196722-240.html?tag=contentMain;contentBody

Zott, C., Amit, R., 2010. Business model design: an Activity system perspective. Long Range Planning, 43, 216-226.

Chapter 9

Appendix: Candidate Organizations for Interviews and Scenario Building

9.1 Healthcare

Following companies / institutions have been identified from the members of the European Health Telematics Association:

1. Alcatel-Lucent (France)
2. CompuGROUP Holding AG (Germany)
3. Coordination Centre for Health Sector Information Systems (Czech Republic)
4. E-health Bulgaria Foundation
5. European Federation of Crohn's & Ulcerative Colitis Associations (EFCCA) (UK)
6. Engineering Sanita Enti Localli (Italy)
7. Gesellschaft für Telematikanwendungen der Gesundheitskarte (gematik) (Germany)
8. HealthSystems Consultants Ltd (United Kingdom)
9. InterComponentWare AG (Germany)
10. KITH – Norwegian Centre for Medical Informatics
11. Maccabi Healthcare Services (Israel)
12. MEDCOM – Danish Centre for Health Telematics
13. MediData AG (Switzerland)
14. Morgan'Conseil (France)
15. NCZI (National Health Information Centre) (Slovakia)
16. NIRS (NHS Information Reporting Services) (United Kingdom)
17. NICTIZ (Netherlands)
18. Norwegian Centre for Telemedicine (NST)
19. Novartis (Switzerland)
20. Odense University Hospital (Denmark)
21. Orange Healthcare (France)
22. SALAR (Sweden)
23. Swedish Rheumatism Association
24. Telegentis (Belgium)
25. The National Institute for Health and Welfare in Finland (THL)
26. VIDAVO (Greece)

27. Vitaphone GmbH (Germany)
28. ZN (Zorgverzekeraars Nederland)
29. ZZZS (Zavod za zdravstveno zavarovanje Slovenije) (Slovenia)

9.2 Public lighting

Following candidates have been identified from the Global Public lighting Federation (GSGF) / and the European Distribution System Operators for electricity (EDSO):

1. Cez Distribuce (Czech Republic),
2. Eandis (Belgium),
3. Endesa Red (Spain),
4. Enel Distribuzione (Italy),
5. Enexis (Netherlands),
6. Erdf (France),
7. Evn (Austria),
8. Iberdrola Distribucion Electrica (Spain),
9. Ores (Belgium), and
10. Union Fenosa Distribucion-Gas Natural Fenosa (Spain).
11. SmartGridIreland

9.3 Cloud Computing in General

The following 264 members of EuroCloud have been sorted randomly:

ADW (Spain)	http://www.adw.es
UniServer	http://www.uniserver.nl/
Altervisions	http://www.altervisions.com/
Oryanoo	http://www.oryanoo.com/
SSAAS	http://www.ssaas.com/
Unitech	http://www.unitech.net/
Epilog d.o.o.	http://www.epilog.net/
Cryptzone	http://www.cryptzone.com/
Telnext srl	http://www.telnext.it/it/
MakeSoft Technologies	http://www.makesoft.es
Magnusson Law	http://www.magnussonlaw.com/
Compubase	http://www.compubase.net/
Eolia Consulting	http://www.eolia-consulting.fr/
BIOS Group	http://www.bios-group.com/
STEEK	http://www.steek.com/
OpenGestion	http://www.opengestion.com/opengestion/index-software-gestion.jsp
NewBase	http://www.newbase.nl/
Elast Office Hungary	http://www.elastoffice.com/hu
eCivilis	http://www.ecivilis.com

Salesforce.com UK	http://www.salesforce.com/uk/
Urcio Aps	http://www.urcio.dk/
Copenhagen Software	http://www.copenhagensoftware.com/
Zylog Systems Ltd	http://www.zslinc.com/
E-Technology	http://www.e-technology.at
IFUA Horváth & Partners	http://www.ifua.hu
CEIT; Central European Institute of Technology	http://www.ceit.at
Mondora	http://mondora.com/
G-DAS	http://www.g-das.hu/
Smartline Systems	http://www.smartline-systems.com/
Twinfield International N.V.	http://www.twinfield.com/
Global SP	http://www.global-sp.net/
Interxion	http://www.interxion.com/
One2Team	http://www.one2team.com/
Parcom d.o.o.	http://www.parcom.si/
Trace One	http://www.traceone.eu/
TricTrac	http://www.trictrac.com/
SafeNet	http://www.safenet-inc.com
Aspire Systems	http://www.aspiresys.com/
Linedata Services	http://www.linedata.com/
INES	http://www.ines.fr/
Sensible Cloud	http://www.sensiblecloud.com/
Steria A/S	http://www.steria.dk/
Studio Moderna d.o.o.	http://www.studio-moderna.com/default_noflash.asp
SineQra Solutions	http://www.sineqra.com/
IPSCA	http://web.ipsca.com/
Equinix	http://www.equinix.com
Quantix	http://www.quantix-uk.com/
Bitport.hu Média	http://www.bitport.hu
DataLogix	http://www.datalogix.nl
HUMANsoft	http://www.humansoft.hu/HUMANsoft_informatika.html
Esker Ibérica	http://www.esker.es
Crayon	http://www.crayon.se/
Progress	http://www.progress.com/fr/
NTC	http://www.ntc.hu
PlanMill	http://www.planmill.com/
LIBRA software	http://www.mve.hu
Claranet	http://www.claranet.es/
Autarcia	http://www.autarcia.com/
Global Network Solution, GNS	http://www.gns.se/
DEYDE Calidad de Datos	http://www.deyde.es
Humiq	http://www.humiq.nl
Workbooks	http://www.workbooks.com/
Secure File Spain	htrtp://www.securefile.es

SAAS IT Consult	http://www.saas-it.net/
STS Group	http://www.group-sts.com/
viaFRANCE	http://www.viafrance.biz/
OCEANET-Technologies	http://www.oceanet-technology.com/
Spamina	http://www.spamina.com
Mamut	http://www.mamut.se/
OODRIVE (France)	http://www.oodrive.fr/
WebAgentur Körbler	http://www.koerbler.com
IDLine	http://www.idline.fr/
Esker	http://www.esker.co.uk/
RESAU Concept	http://www.reseau-concept.com/
D2C	http://d2c.org.uk/
Microsoft Hungary	http://www.microsoft.com/hu-hu
Dragø Kommunikation	http://www.dragoe.net/
NetApp Hungary	http://www.netapp.com/as/contact-us/?c=y&3767=187036
Haude electronica Verlags-GmbH	http://www.haude.at
Sayit SA	http://www.sayit.ch/
Geo Networks Limited	http://www.geo-uk.net/
iMotion International	http://www.i-motion.hu
Insight	http://www.insight.com/
ASP64	http://www.asp64.com/
LiveOffice	http://www.liveoffice.com/
FAW Institut	http://www.faw.at
Loginor	http://www.loginor.qc.ca/
XYMOX	http://www.xymox.fr/
France Telekom	http://www.francetelecom.com/
Toluna	http://www.toluna.com/
EMC	http://www.emc.com/
Webstudio	http://www.webstudio.es/
C Infinity	http://www.cinfinity.co.uk/
NTRGlobal	http://www.ntrglobal.com/
Delógica	http://www.delogica.com/
Edisonweb srl	http://www.edisonweb.com/en/
2C Change	http://www.2cchange.com/
Réti, Antall Partners PwC legal office	http://www.landwellglobal.com/hu
Comptanoo	http://www.comptanoo.com/
Webstudio	http://www.webstudio.es/
CloudCredentialCouncil	http://www.cloudcredential.org
KYRIBA	http://www.kyriba.com/
BeesNEST	http://www.beesnest.fr/
Abesse	http://www.abesse.hu
Changefirst Ltd	http://www.changefirst.com/
RISC Group	http://www.risc-group.com/
e-PAYE	http://www.e-paye.com/
Inter Online Cooperación	http://www.eurocloudspain.org/es/inter-grupo

Flying Servers	http://www.flyingservers.eu
CEGID	http://www.cegid.fr/
DLA Piper Hungary	http://www.dlapiper.com/hu-HU/hungary
Astec d.o.o.	http://www.astec.si/
The Siemon Company	http://www.siemon.com
Blue Monkeys GmbH	http://www.bluemonkeys.at
Eptisa Tecnologías de Información	http://www.ti.eptisa.com
FlexxibleIT	http://www.fexxibleit.com
GiMiScale	http://www.gimiscale.com
e-MOTION	http://www.upsale.fr/
SAP	http://www.sap.com/
Passwordbank	http://www.passwordbank.com/
Webroot	http://www.webroot.co.uk/En_GB/business.html
Spica International d.o.o.	http://www.myhours.com/
Servoy	http://www.servoy.com/
VMengine	http://www.vmengine.net/
EBRC	http://www.ebrc.com
MyGestion	http://www.mygestion.com
NTT Europe Online	http://www.ntt.eu
Virtua d.o.o.	http://www.virtua.si/
Generix	http://www.generix.fr/
Fujitsu Hungary	http://www.fujitsu.com/hu
GESIO SOLUTIONS S.L.	http://www.gesio.com
Kendox AG Niederlassung Österreich	http://www.kendox.com
Ctac	http://www.ctac.nl
Ilait	http://www.ilait.com/
NEXON	http://www.nexon.hu
Liland IT GmbH	http://www.lilandit.com
SOURCIA	http://www.sourcia.com/
Procullux Ventures	http://pcxvs.com/
Andréewitch and Simon	http://www.andsim.at
Hoellwarth Consulting	http://www.hoellwarth.at
ReasonNet	http://www.reasonnet.com
SFR Business Team	http://www.sfrbusinessteam.fr/nos-solutions/services-herberges/index.jsp
Segura Duran Assessors	http://www.sd-a.com
Terremark (Netherlands)	http://www.terremark.nl
LuxCloud	http://www.luxcloud.com/
Baermann KM	http://www.bkmsaas.com/
Proginov	http://www.proginov.com/
Vedior Front RH	http://www.vediorfrontrh.com/
TMForum	http://www.tmforum.org
Microsoft	http://www.microsoft.com/softwareplusservices/
Clever Technologies	http://www.clever.fr/
Xlab d.o.o.	http://www.xlab.si/index-en.html
ITESOFT	http://www.itesoft.com/

OVH HISPANO	http://WWW.OVH.ES
Ikarus security software GmbH	http://www.ikarus.at
Edatis	http://www.edatis.com/
Oodrive (Spain)	http://www.oodrive.es
Central Europe On-demand	http://www.ceondemand.com
Citrix Systems GmbH	http://www.citrix.at
Arsys	http://www.arsys.es/
Basefarm	http://www.basefarm.se/
Salesforce	http://www.salesforce.com/eu
Intevo websolutions GmbH	http://www.intevo.net
Zyncro	http://www.zyncro.com
Alpineon d.o.o.	http://www.alpineon.com/
TribalOS	http://www.tribalos.com
Unit 4	http://www.unit4.nl/
JNovapoint GmbH	http://www.jnovapoint.com
Arctur d.o.o.	http://www.arctur.si/
Projectplace International	http://www.projectplace.com/
WebLookOn GmbH	http://www.weblookon.com
SAP (UK) Ltd	http://www.sap.co.uk/
RAN NETWORKS S.L.	http://www.ran,es
ASPlenium Logix	http://www.asplenium.fr/
Acros d.o.o.	http://www.acrossecurity.com/
Event Catalyst	http://www.catalyst.fr/
Commvault	http://www.commvault.com/
Programshop	http://programshop.com/
GTS Hungary	http://www.gts.hu/
RunMyProcess	http://www.runmyprocess.com/
Exthex GmbH	http://www.exthex.com
House of Ports	http://www.ports.se/
Esker Italia srl	http://www.esker.it/
Crypto	http://www.crypto.fr/
InterGrupo	http://www.intergrupo.net
E-conomics	http://www.e-conomic.dk/
Witsbits	http://www.witsbits.com/
KEYCLOUD (APGISA)	http://www.apgisa.es
Cotranet	http://www.cotranet.com/
Aner	http://www.aner.com
Midrange	http://www.midrange.fr/
Cloud Vision	http://cloudcomputing-vision.com/
VMWare Hungary	http://www.vmware.com/company/office_hungary.html
NextApplication	http://www.nextapplication.fr/
IS Tools	http://www.istools.com/
Puaschitz IT Individuelle IT lösungen	http://www.puaschitz.at
ITEANU	http://www.iteanu.com/

MAPI	http://www.mapi.hu
Selligent	http://www.selligent.com/home.asp?lg=fr
Kuadriga Aps	http://www.eurocloud.org/www.kuadriga.com
VMWare	http://www.vmware.com
Dutch Hosting Providers Association (DHPA)	http://www.dhpa.nl
WatchGuard Technologies, Inc.	http://www.watchguard.com/
Pawn Promotion	http://www.pawnpromotion.com/
Litebi	http://www.litebi.com/
WayCast	http://www.waycast.info/
Genis d.o.o.	http://www.genis.si/genisweb
Centerstone	http://www.centerstone-europe.com/
Personal Consult Strategic cloud business advisors	http://www.personalconsult.nl/
Mimecast	http://www.mimecast.com/
University of Ljubljana; Faculty of computer and information science	http://www.fri.uni-lj.si/en/
Atrox Development	http://www.atrox.se/