Katrin Riemer

Digital Signature Service in the Cloud

Master thesis

to achieve the university degree of

Diplom-Ingenieur

Software Engineering and Management

submitted to

Graz University of Technology

Adviser: Ass.Prof. Dipl.-Ing. Dr. techn. Christiana Müller
Auditor: Univ.-Prof. Dipl.-Ing. Dr. techn. Stefan Vorbach

Institute of General Management and Organization

Graz, January 3, 2017

EIDESSTATTLICHE ERKLÄRUNG

AFFIDAVIT

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt, und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Das in TUGRAZonline hochgeladene Textdokument ist mit der vorliegenden Masterarbeit identisch.

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present master‘s thesis.

Datum / Date

Unterschrift / Signature

Acknowledgment

I would like to express my gratitude to the head of the institute of general management and organization Univ.-Prof. Dipl.-Ing. Dr.techn. Stefan Vorbach, that it was possible to write this master thesis at the institute and my supervisor at the institute Dipl.-Ing. Dr.techn. Christiana Müller for the useful hints and for answering all my questions.

At this point I would also like to thank the company *XiTrust* for giving me the possibility to write a master thesis at the company and about a topic I am really interested in. Furthermore, I would like to thank the whole team for explaining everything to me and for answering all my questions throughout the last months.

Also, I like to thank the participants of my expert interview, who have shared their specialist knowledge and their valuable time during the process of interviewing.

Kurzfassung

Diese Masterarbeit beschäftigt sich damit, eine digitale Unterschriftenmappe als Cloud Service anbieten zu können. Bei dieser Unterschriftenmappe handelt es sich konkret um das Produkt *XiTrust MOXIS*, vom Unternehmen *XiTrust Secure Technologies GmbH*. Die Herausforderung dabei liegt vor allem darin, dass wichtige Dokumente die jeweiligen Unternehmensgrenzen verlassen würden und trotzdem die Integrität, die Authentizität und die Vertraulichkeit gewährleistet werden können. Die Herausforderung ist dabei nicht die technische Realisierung, sondern viel mehr gilt es dabei auch organisatorische und rechtliche Aspekte zu berücksichtigen, um den Kunden wirklich von dieser Lösung überzeugen zu können.

Aus diesen Gründen wurden Literaturrecherchen und mehrere Experteninterviews mit bestehenden aber auch potentiellen Kunden geführt. Außerdem konnten durch die enge Zusammenarbeit mit den Mitarbeitern der Firma *XiTrust* wichtige Anforderungen und notwendige Meilensteine für die Umsetzung gewonnen werden. Zusätzlich dazu wurden nach durchlaufen eines iterativen Prozesses zwei Geschäftsmodelle erstellt. Eines der Geschäftsmodelle bildet dabei die generelle Anwendung von *XiTrust MOXIS* in der Cloud ab, während sich das andere Geschäftsmodell auf den Krankenhausbereich fokussiert. Um ein gesamtheitliches Bild zu bekommen, wurden weitere Methoden, wie eine *Service Lifecycle Map* und *Value Maps and Customer Profiles* verwendet. Darüber hinaus wurde auch das Umfeld der Geschäftsmodelle mit Hilfe der *Business model environment* Analyse von *Osterwalder und Pigneur* begutachtet.

Das Ergebnis dieser Masterarbeit zeigt, dass die digitale Unterschriftenmappe *XiTrust MOXIS* als Signaturservice in der Cloud realisiert werden kann. Um den jedoch rechtlichen, technischen und organisatorischen Anforderungen Folge zu leisten, müssen noch einige Maßnahmen getroffen werden. Diese Maßnahmen wurden in dieser Masterarbeit festgehalten und eine zeitliche Abfolge der zu erreichenden Meilensteine wird vorgeschlagen.

Abstract

This master thesis deals with an electronic signature file that should be provided in the cloud. This electronic signature file is a product of the company *XiTrust Secure Technologies GmbH* and is called *XiTrust MOXIS*. The challenge of providing such a product in the cloud is to ensure the integrity, authenticity and confidentiality of important documents with sensitive data, which will leave the internal IT infrastructure of the customers. Furthermore, organizational and legal requirements also need to be considered in order to convince customers to buy this product.

For these reasons, an intensive literature research has been conducted and expert interviews with established customers as well as with potential customers were held. Due to the close cooperation with the employees from *XiTrust* many important requirements and milestones could be defined. Additionally, two business models have been developed through an iterative process. One of these business models covers the general case of providing *XiTrust MOXIS* in the cloud and the other covers the hospital area. Furthermore, methods such as the *Service Lifecycle Map* and *Value Maps and Customer Profiles* have been used to gain a complete picture. Moreover, the environment of the business models has been examined, as it is suggested by *Osterwalder and Pigneur*.

The result of this thesis shows, that it is possible to the provide the electronic signature file *XiTrust MOXIS* in the cloud. In order to realize this, the technical, organizational and legal requirements need to be fulfilled and the recommended measures have to be taken. Additionally, also some milestones that need to be reached including the sequencing of these milestones are provided.

Contents

Figures

List of abbreviations

AWS	Amazon Web Services
CASB	Cloud Access Security Broker
CRM	Customer Relationship Management
CSP	Cloud Service Provider
DDoS	Distributed Denial of Service
DMS	Database management system
DTM	Digital Transaction Management
EC2	Elastic Compute Cloud
ECS	Enterprise Cloud Subscribers
eID	electronic Identity
ERP	Enterprise Resource Planning
GAE	Google App Engine
HRM	Human Resource Management
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PGP	Pretty Good Privacy
PKI	public key infrastructure
RO	Registration officer
RTR	Rundfunk & Telekom Regulierungs-GmbH
SaaS	Software as a Service

SAML	Security Assertion Markup Language
SLA	Service-Level-Agreement
SSO	Single Sign-on
UI	User Interface
VPN	Virtual Private Network
WS-Federation	Web Services Federation

1. Introduction

More and more companies are using cloud services and therefore the cloud infrastructure sales account for over 25% which is almost $6.3 billion in the first quarter of 2015 (IDCResearch, 2015). A forecast, regarding the growth of cloud-based platforms, states that more than 60% of all companies will have at least 50% of their infrastructure in a cloud (Mcnee, 2014). The Computerworld Forecast Study (2015) figured out that cloud computing projects are the most important projects in 16% of the IT departments that were surveyed. On the second place are legacy systems with 12% and on the third software on-premises with 9%. Further, 42% of the companies said that they will increase their spendings on cloud computing. (Columbus, 2014) The leader in this market is by far Amazon, followed by Microsoft. All the other cloud service providers lie far behind these two. (Maguire, 2015)

1.1. The company XiTrust Secure Technologies GmbH

The company *XiTrust Secure Technologies GmbH* was founded in 2002 and provides software solutions, which guarantee to process documents without media disruption. *Xitrust* is an ambitious, innovative company which is always interested in new trends and as the cloud sector is becoming more popular, they also want to start providing their services in the cloud. A lot of companies print their documents in order to sign them in conformity with the law, with a handwritten signature. Afterwards, the documents get digitalized again to be able to archive the documents digitally. This is very expensive and time consuming for those companies. Therefore, *XiTrust* offers customized solutions which enable the processing of documents without media disruption. These customized solutions can be really diverse as the customers of *XiTrust* come from different areas in the economy, from the healthcare sector as well as from the public sector. For this reason, *XiTrust* implements their products modular to be able to provide a complete package for their different customers, starting from picking up the files from somewhere in the file store to delivering the signed document to the receiving person. This whole process is covered by the following products (Aschbacher, 2014):

- XiTrust MOXIS
  XiTrust MOXIS is the electronic version of a traditional paper-based signature folder. This saves a lot of time and money because people do not need to run around getting all the

signatures and if these documents need to be archived they do not need to print, sign and scan them. In order to sign a document with *XiTrust MOXIS*, the mobile phone signature, the Austrian citizen card and other signature cards can be used. These signatures are based on qualified certificates issued by a certified trust center and are called qualified signatures. A qualified signature is by law legally equal with the handwritten signature. Additionally, *XiTrust MOXIS* is a web-based application and can, therefore, be accessed from every PC and every mobile device without installing additional software. Together with the mobile phone signature it is possible to sign everywhere and any time. Not only one document at the time can be signed, with *XiTrust MOXIS* it is also possible to sign many documents at the same time. Further, it is also possible to electronically invite many people to sign one document, which means that documents that need to be signed by many people can be signed within a few minutes.

- XiTrust Business Server
  The *XiTrust Business Server* is the solution for signing, encrypting and managing documents. This specifically includes signing, examining and archiving invoices and it is also possible to sign documents directly in the workflow-system. This means that the user does not realize that he/she is using a different system when he/she is signing a document. The *XiTrust Business Server* can be directly integrated in the customers system and offers interfaces to e-mail servers to secure e-mails and to different other services such as SAP or MS Sharepoint.

- XiTrust Time stamp Server
  The *XiTrust Time stamp Server* attaches an electronic time stamp to a document in order to guarantee the authenticity of the document at the moment when the stamp was attached. This is particularly useful for time critical documents such as tenders, patents and documents which are legally relevant. The *XiTrust Time stamp Server* attaches these time stamps not only to documents but also to e-mails so that it is documented clearly when the electronic information has reached the company.

1.2. Objectives of the thesis

As the company *Xitrust* wants to expand their market reach, they want to provide their product *XiTrust MOXIS* in the cloud. A further advantage for the company is that they would save time because now they have to install their software into the clients infrastructure. This is not a very scalable approach and, therefore, they would like to provide *XiTrust MOXIS* in the cloud. As they are working with highly sensitive data, a lot of things need to be considered before the step into the cloud area is possible.

The objective of this thesis is therefore, to come up with organizational, technical and legal requirements, a business model and measures that are needed, to implement *XiTrust MOXIS* in the cloud. For this reason, an exhaustive research will be conducted in terms of which approaches already exist regarding signature services, identity management services and ehealth services in the cloud across Europe. In a next step all the requirements that need to be fulfilled will be gathered through an exhaustive signature service as well. In addition, value maps, customer profiles, a service lifecycle map and also a business model will be developed. During this development, the following two workflows need to be considered:

- Hospital workflow one: A doctor is signing a patient's record
- Hospital workflow two: The hospital administration and the patient are signing a document together.

The goals of this thesis do not include an implementation of *XiTrust MOXIS* in the cloud nor a prototype needs to be created.

1.3. Methods

The first phase also called *research phase* was dominated by information gathering and getting an first overview of all the relevant topics to provide *XiTrust MOXIS* in the cloud. For this reason the main methods that have been used were the literature review and the expert interviews. A literature review was conducted for the definitions of cloud computing, the business model and the service lifecycle map. Furthermore, the information regarding the legal basics for electronic identification and transactions and the process of identity provisioning were gathered by a literature research. All the information (see chapter *Analysis of Existing Approaches for Services in the Cloud*) was also gained through an intensive research. Last but not least, also the requirements and the different milestones were partially elicited through a literature review. The expert interviews belong to qualitative research methods and were used to gain requirements and knowledge about the environment of the general business model.

In the next phase also called *business model phase* the information that had been gathered in the first phase were used to implement a value map and customer profile as well as a business model. In a next step the first versions of a value map, customer profile and a business model were discussed during a workshop with the supervisors from the university and from *XiTrust*. The main reason why this workshop was held was to get a feedback for the first versions but also to develop a better understanding of the business model canvas. After the workshop a new iteration of establishing value maps, customer profiles and business models has been started and after every iteration a feedback was given by the supervisors. Besides that the business model environment and a service lifecycle map has been defined in an iteratively process as well. The information was thereby gained from the interviews and from different talks with the employees from *XiTrust*.

The third phase was the *requirements specification phase* where all the information that has been collected through out the literature review, the expert interviews but also the knowledge that has been gained through the implementation of the business model and so on was written down as requirements.

Last but not least the phase *composition of master thesis* in which all the information has been combined and written down in this thesis. This whole process is shown figure 1.

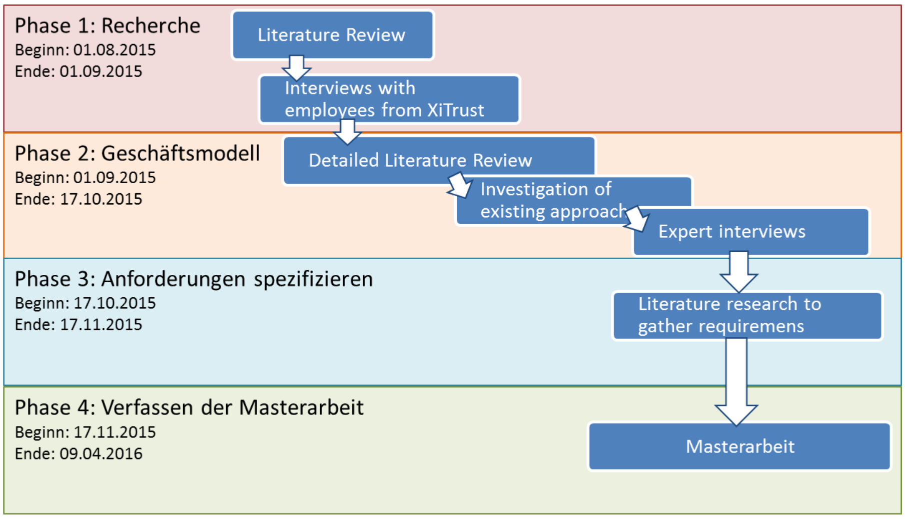

Figure 1.: Chronology of the used methods and approach of this thesis (own illustration)

1.4. Structure

- In chapter two, all the theoretical terms that are used throughout this thesis are explained. The terms reach from cloud computing via the service lifecycle map and the business model to how a person can get a hard eID and what regulations are in place to sign documents from all over Europe with this hard eID.
- In chapter three, different existing approaches are presented. At the beginning of this chapter a research project from Germany that deals with a secure identity management in a cloud context is described. Thereafter, three projects funded by the European commission are described which focused on cross-border interoperability between the eHealth systems of different European countries, on establishing a single European electronic identification and authentication area and on securing services in these areas in general. Furthermore, three companies that work in the digital signature and electronic identity management area are presented. The first one, called *PrimeSign* is a smaller company which is located in Graz and focuses on electronic signatures. The other two are called *OPENTRUST* and *DocuSign* and

are much bigger. While *DocuSign* is mainly focusing on digital signatures, *OPENTRUST* is mainly focusing on identity management.

- The fourth chapter captures the approach of the practical part. The first method that has been used were expert interviews followed by customer profiles and value maps that have been created to gain some good insights for the development of the business models.
- In chapter five, the elicited requirements are then presented which have been categorized into technical, legal and organisational requirements.
- In chapter six, the practical results of this thesis are presented. These results include the answers of the expert interviews, the description of the business model environment, the general business model and the eHealth domain business model for *XiTrust MOXIS* in the cloud.
- In chapter seven, the recommended actions are then presented that need to be made in order to provide *XiTrust MOXIS* in the cloud.
- Last but not least, a summary of this thesis and possible future work is provided in chapter eight.

Part I.

Literature Review

2. Theoretical Foundations

In this chapter, an example of the definition of cloud computing is given and the major cloud service providers are described. Thereafter, a brief description of the service lifecycle map is given and also the business model canvas as it is defined by *Osterwalder and Pingeur* is presented, including the presentation of all the nine building blocks. As the business model cannot be completely separated from the environment, a definition of the business model environment is also provided. The environment is thereby split up into four areas as suggested by *Osterwalder and Pingeur*. Furthermore, a short summary of the *eIDAS* regulation is given as this regulation enables people, who have a hard eID, to use the mobile phone signature all over Europe. Hard eIDs are identities, that are based on qualified certificates and are made for identification and authentication purposes at a high assurance level. Last but not least, the process of getting such a hard eID is described by the example of how it works in Austria.

2.1. Cloud Computing

A general definition of cloud computing is problematic, as it is a huge pool of resources with different technologies and different configuration probabilities. Furthermore, different kind of services can be provided and the cloud system can be deployed with different scopes. However, one possible definition of cloud computing is provided by the NIST publication *Special Publication 800-145* (Badger et al., 2011):

> „*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.*“

These five essential characteristics are the following (Badger et al., 2011):

- On-demand self-service: This means that the customer of a cloud service can allocate as many computing resources as he/she needs without human interaction.

- Broad network access: This means that the customer can access the resources of the cloud service provider through standard mechanisms over the network.
- Resource pooling: This means that all the computing resources of the provider are pooled and dynamically assigned and reassigned to the customer according to his/her demand. The customer does not know nor has control over where the resources are located.
- Rapid elasticity: This means that the resources can be provisioned rapidly and elastically. Therefore, the resources appear to be unlimited for the customer.
- Measured service: This means that the amount of resources used can be monitored, controlled and reported so that the provider and the customer know how many services and how much the services have been used.

The three service models mentioned above are defined as follows (Badger et al., 2011):

- Software as a Service (SaaS): The user can use the applications from the cloud service provider via a thin client interface such as a web browser or a program interface. The underlying cloud infrastructure, network, servers, operating system, storage or even individual application capabilities are thereby not managed by the user.
- Platform as a Service (PaaS): The user can deploy applications. The underlying cloud infrastructure, the network, the server operating system and the storage are thereby not managed by the user but he/she can at least control the deployed applications and the environment where the applications are hosted.
- Infrastructure as a Service (IaaS): The user gets some processing power storage and other fundamental computing resources and on this resources the user can install and run operating systems and applications as he/she wants. The underlying cloud infrastructure is, however, not managed by the user.

Last but not least, the four deployment models are the following (Badger et al., 2011):

- Private cloud: A private cloud is a cloud where all the resources in this cloud can only be used by the people of one organization. The management of the cloud can be carried out by this company, a third party or they do it together. The cloud can be on or off premise.
- Community cloud: A community cloud is a cloud that consists of companies which have the same concerns regarding a topic, for example security. This means that only the employees from these companies can use the cloud. The management of the cloud can be carried out by one or more members of this community, by a third party or they do it together. The cloud can be on or off premise.
- Public cloud: A public cloud is a cloud where everybody can use the resources of this cloud. The management of the cloud can be carried out by a government, an academic, a business or they somehow do it together. The cloud is on the premise of the cloud provider.
- Hybrid cloud: A hybrid cloud is a cloud that consists of at least two different kinds of clouds (private cloud, community cloud, public cloud). The different clouds are thereby connected with a standardized technology or with their own technology, so that applications and data can be exchanged.

One of the reasons why cloud computing is becoming more and more popular are the reduced costs because the consumer simply pays for the amount of services used. Another advantage is that the consumer can access his/ her applications/information wherever they are, without using additional software. This increases the mobility, the portability of application and the ease of use. Despite these advantages, a few security issues need to be considered before using cloud services. Especially the user privacy and sensitive data of critical enterprise applications are topics that need to be taken care of. (Srinivasan et al., 2012)

Even though there are many obstacles, cloud computing is becoming more and more popular as the pay-as-you-go principle is very convenient. Figure 2 shows IaaS providers that are still niche players and providers that are already leaders in that area.

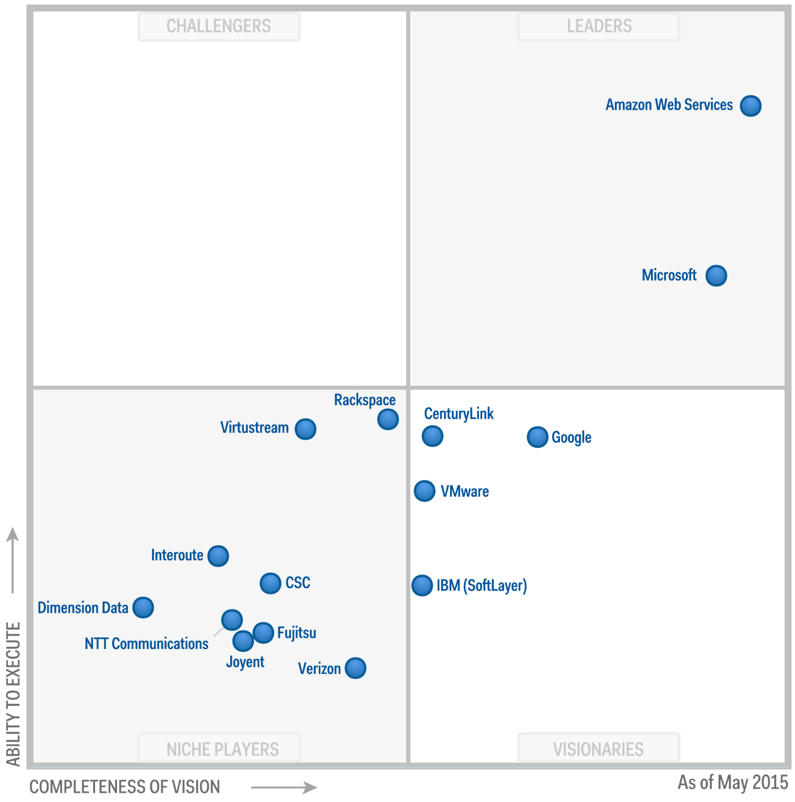

Figure 2.: Magic quadrant of IaaS provider (Leong et al. (2015))

The biggest players in this area are at the moment:

- Amazon Web Services (AWS)
  In 2006, *Amazon* started with its *Simple Storage Service (S3)* and the *Elastic Compute Cloud (EC2)*. One reason that made *EC2* so successful was the fact that *Amazon* gave their customers plain virtual machines and did not restrict them within their virtual machines which made them feel as if they work on their local computers. (Metz, 2012) Beside the fact

that *Amazon* did not restrict their customers within their virtual machines, another advantage of the *EC2* is that the customers do not need to worry about the underlying infrastructure such as the network or the storage. (Morgan, 2014) *Amazon* is located at many places all over the world and this means that they have a diverse customer base. *AWS* has over 10 times more cloud IaaS computing capacity than the next 14 largest cloud service providers together. This made it possible to attract many technology partners which further enables *AWS* to be very innovative, agile and responsive to the market. They expand their offers very quickly and therefore have the biggest spectrum of IaaS features and PaaS-like capabilities. (Maguire, 2015)

- Microsoft Azure
  Microsoft entered the cloud market in 2008 with *Microsoft Azure* (Qian et al., 2009). *Microsoft Azure* consists of *Windows Azure, SQL Azure* and *Azure AppFabric*. *Windows Azure* provides scalable storage space and on-demand computation of cloud applications. *SQL Azure* provides a database with additional capabilities in comparison to a normal SQL Server. *Azure AppFabric* provides a set of .NET Services. (Sultan, 2011) *Microsoft Azure* is a PaaS provider and is the most important part of *Microsofts hybrid cloud (Cloud OS)*. Cloud OS combines Microsoft Azure, Windows Server, Microsoft System Center and the public cloud. Furthermore, Microsoft Azure can be accessed from every end-user device as it is does not rely on the underlying hardware configuration. (Shields, 2014)

- IBM SmartCloud
  IBMs SmartCloud includes infrastructure as a service, platform as a service and software as a service solutions. All these different kinds of services can be offered through a public, private or hybrid cloud. These offers are covered by the following three solutions: SmartCloud Foundation, SmartCloud Services and SmartCloud Solutions. (IBM, 2015) IBM started in 2007 to develop a cloud strategy. The goal of their cloud computing strategy was to serve enterprise customers and to close the gaps of existing cloud environments. IBM teamed up with Google in the same year in order to distribute information about cloud computing at universities. Four years later the IBM cloud solution named SmartCloud began to grow in a steady manner. In the same year IBM announced that already 400 companies use their cloud solution. (IBM, 2013)

- Google Cloud Platform
  Google released their Google App Engine (GAE) in 2008 (McDonald, 2008). Google App Engine is a PaaS solution and enables the user to develop applications. All applications are sandboxed and can, therefore, run in a safe environment. (Google, 2015a) A real competitor to Amazons S3 cloud storage is the Google Cloud Storage, because Google also offers their customers to store their data on Google's infrastructure which has a very high reliability, availability and a very good performance (Google, 2015b). After the release of Google Cloud Storage, Google introduced the Google Cloud Platform which consists of many different

cloud services. These services are thereby split up in these categories: Compute, Storage, Big Data, Services and all cloud services are assigned to theses categories. (Google, 2015c) For deploying large scale software it is important to consider that a manual configuration will result in a maintenance challenge. For customers who use Google App Engine this is already managed by GAE but for the other customers, Google developed the Google Cloud Deployment Manager which makes designing, sharing, deploying and managing complex cloud solutions easier. (Joneja, 2014)

2.2. Service Lifecycle Map and Business Model

In this section a service lifecycle map is presented, which describes all the different needs that customers have when they want to buy a product or service and also the services that companies offer to satisfy customer needs. Furthermore, value maps and customer profiles are described as they offer a great possibility to visualize the pains, gains and jobs of customers and all the products/services, gain creators and pain relievers a company can offer. Moreover, it is also defined what a FIT between the customer profile and the value map is. Last but not least, all the building blocks of the business model canvas are described.

2.2.1. Service Lifecycle Map

The goal of the service lifecycle map is to point out the services which serve the different needs of the customer best and so the company gains a competitive advantage. Another advantage is that it provides a good overview of the services that a company already offers and therefore, it shows also in which phases of the service lifecycle map additional services would be needed. The service lifecycle map is used to visualize the phases a customer is going through when he/she is buying a product or service. The service lifecycle map is displayed in figure 3 and divided into the following four phases: The first phase is the information phase. This is the phase where the customer tries to get the right information of the product he/she is interested in. The second is the offer and purchase phase. This is the phase where the customer wants to get more specific information about the product and also about the costs of it. The third phase is the order and execution phase. The customer has now already ordered the product and therefore, the usage of the product needs to be prepared in this phase. Last but not least, the fourth phase this is the use phase and so it is very important to offer supporting services for the usage and possibly make further offers. If a company develops a product, the customer is less involved in the development process than if a company renders a service. Services can further be split up into personalized and knowledge intensive services. For the personalized services the presence of the customer is mandatory, while he/she simply provides information for the the knowledge intensive services. The service lifecycle map is especially useful to display the contacts between the customer and an employee from the company. Meetings can be in different phases, in which the customer has different needs and, therefore, the employee needs to offer different services. (Harms et al., 2009) The service lifecycle map can be used by every company that fosters business-to-consumer relationships as all these companies offer some kind of service for their consumers.

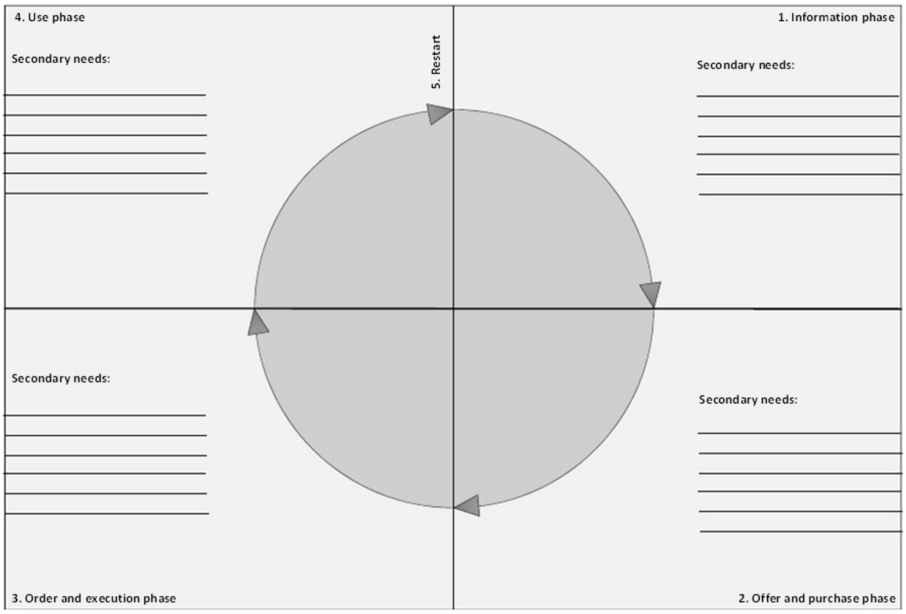

Figure 3.: Service lifecycle map (Aschbacher (2014))

2.2.2. Business Model Canvas

There exist many different definitions of a business model but *Hoppe and Kollmer* suggested a definition already in 2001. A business model in their definition, is a simplified illustration of a company that is aiming at profit. (Hoppe and Kollmer, 2001)
For *Amit and Zott* is the business model, the design of the transaction content, the structure and the management, with the goal to create value by using business opportunities. (Amit and Zott, 2001)
Osterwalder and Pingeur defined a business model as follows: „*A business model describes the rationale of how an organization creates, delivers and captures value.*“ (Osterwalder and Pigneur, 2010)
Hamel presented already in 2001 four elements of a business model, that can also be found in the business model definition of *Osterwalder and Pigneur*. He introduced the customer interface, which can be mapped to the customer segment from *Osterwalder and Pigneur*. Furthermore, the main strategy, which is displayed in the value proposition block of *Osterwalders and Pigneurs* business model. The next elements are the strategic resources, which are similar to the key resources in the business model canvas from *Osterwalder and Pigneur* and the value network, which

can be compared with the key partners from *Osterwalder and Pigneur*.
These are just a few business model definitions but it shows, that business models can be seen quite differently on the one hand but on the other hand some definitions also show similarities as the example with *Hamel* and *Osterwalder and Pigneur* shows. (Schallmo, 2013)

Osterwalder argues in his PhD thesis that the reason why the concept of business models had become so popular is that managers simply have too many choices. They have many different opportunities when it comes to how customers can be reached or when they have to define their value proposition and this concerns also many other decisions. Further, the fact that science and technology have experienced a huge progress in the last years, increased the competition between companies. Companies are, therefore, using two means to gain profit. The first mean is that they try to reach new markets by introducing a new product/service or by geographical expansion. The other mean is to use new technologies and gain new skills to reduce costs. (Osterwalder, 2004)
Furthermore, *Hodgson* mentions that services are more diverse than manufactured goods and also that the service sector is increasing. This means that also the diversity increases. These are the facts, why managers have much more choices but also much more decisions to make, regarding their business models. (Hodgson, 2003)

Osterwalder mentions that also the placement of the business model is very important as it is the mean to set up a logic with which the company is able to earn money. He further mentions, that the business model can operate as a conceptual link between strategy, business organization and ICT. These three worlds are very different and, therefore, understanding gaps can occur. The business model concept could function as a glue in this situation but to implement the business vision, the company needs to communicate the concept very clear as different people with different perspectives need to cooperate for the implementation. *Osterwalders* suggestion is to use the business model for supporting managers to provide a clear picture of the business strategy for them and for others as well as to create and change the strategy if necessary. Business models might, therefore, be the difference when it comes to management with uncertainty. (Osterwalder, 2004)

As the market is getting more competitive it is not enough for companies to focus on product and process innovations and, therefore, a lot of companies started to innovate their business models. Furthermore, *business model innovations* have definitely a higher success potential, regarding empirical results. (Gassmann and Csik, 2013) For this reason the interest in business model innovation increases but many people are still uncertain what a business model innovation really is. One reason for this might be that there exist many different definitions of a business model. For some people business model innovation is only the innovation of a few elements/blocks of the model while it is the innovation of a complete business model for others. (Morris et al., 2005) (Marko, 2014)

While technology innovations became normal in the last years, business model innovations are far away of that, even though they are at least equal or even more important. Nevertheless, it is a fact that a company can only increase their capacity if they have enough capacity to create new business models. Another fact that is shown by history is that, if a company cannot provide a satisfying value proposition to their customers and they cannot create a business system that delivers the required quality at a good price, the innovator will fail, no matter how good the innovation was. This shows that management, entrepreneurship, business model design and implementation is as important as technological innovation in order to achieve economical growth. In order to stay competitive in these times it is very important for companies to seek and consider improvements of their business model on a regular basis. These improvements should add value for customers and are ideally hard to imitate. Even tough a change of the business model might have some disadvantages, it is always better to initiate such a change itself than the company gets forced to do it by external events. (Teece, 2010)

The business model definition that was followed in this thesis is the one from Osterwalder and Pigneur (2010): „*A business model describes the rationale of how an organization creates, delivers and captures value.*“
In order to show how a company creates value with a product or service in a compact way, *Osterwalder and Pingeur* developed the business model canvas. They divided their business model into nine building blocks and display them on one page as shown in figure 4. (Osterwalder and Pigneur, 2010)

1. **Customer Segments**
   The customer segments block represents all the customers that a company wants to serve with one product. The customers may either be represented by one big segment or a few small segments. In order to perfectly serve the different customers they should be split into groups regarding their needs. Each customer group must thereby see a benefit for themselves in the the value proposition of this Business model.

2. **Value Propositions**
   The value proposition block describes which values the company provides with one of their products or with one of their services for the different customer segments. The value propositions solve the problems of a customer and based on the propositions of a company, a customer decides from which company he/she wants to buy. These value propositions can either be completely new or they add some value to an already existing proposition.

3. **Channels**
   The channels describe how a company gets and stays in contact with its customers. In the *service lifecycle map* the contact points between the company and the customer are visualized with dots and those meeting points are represented by the channels block in the business model canvas. (Aschbacher, 2014) These channels are used to raise the awareness about products and services, to evaluate the value proposition, to sell products and services, to deliver the value proposition to the customer and to support customers when they use a product or service.

4. **Customer Relationships**
   The customer relationship block defines, what type of relation the company has with a customer segment. These relationships are build to acquire customers, to bind the customer to the company and to convince customers to buy more expensive products (upselling). The relationship between a customer and a company can range from personal to automated and has a huge impact on the customer experience.

5. **Revenue Streams**
   The revenue streams represent the amount of money that the customer has to pay for a value proposition. The pricing model can be different for every revenue stream and can range from asset sale to licensing or advertisement. In general, revenues can be divided into transaction revenues that result from one time purchases or recurring revenues which can be received from ongoing purchases. Furthermore the pricing mechanism can either be fixed which means that the prices are based on static variables or dynamic which means that prices are constantly changed by market conditions.

6. **Key Resources**
   The key resources block lists all the resources that a company needs, to create and deliver a value proposition for a customer segment and to stay in contact with the customer segments. Depending on the type of a company, the key resources can vary strongly because while a manufacturing company needs a lot of machines, a consulting company needs more human resources.

7. **Key Activities**
   As well as the key resources, key activities are necessary for a company to be able to create and deliver a value proposition. Furthermore, key activities are also different for different types of companies. The key activities can be divided into production, problem solving and platform/network.

8. **Key Partnerships**
   The key partners are all companies that need to work together in order to successfully create and deliver the value propositions of this business model. The reasons why companies establish partnerships can be different, for example optimization might be one reason while another might be to mitigate risks or to simply purchase resources. Furthermore, key partnerships can be of four different types:

   - Strategic alliances: Between non-competitors.
   - Coopetition: Strategic partnerships between competitors.
   - Joint ventures: To establish a new business.
   - Buyer-supplier relationship: To ensure reliable supplies.

9. **Cost Structure**
   The cost structure represents all the expenses that need to be made in order to run a business model. For some business models, a low cost structure is more important than for others and, therefore, the cost structure can be divided into value driven and cost driven cost structures. (Osterwalder and Pigneur, 2010)

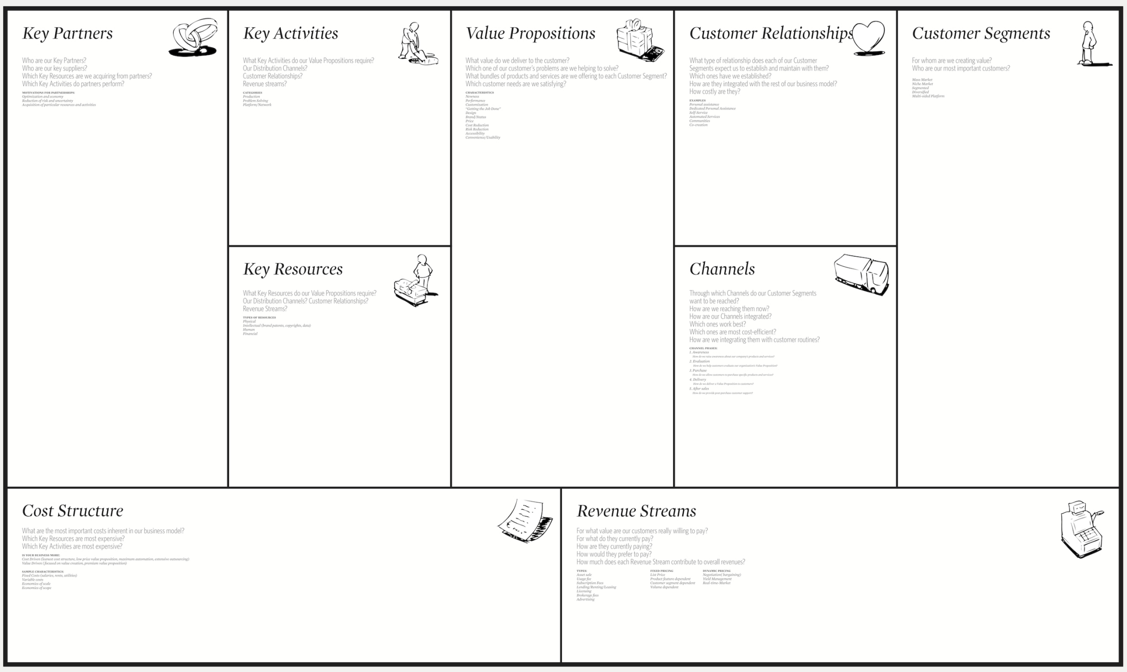
Key Partners
Who are our Key Partners?
Who are our key suppliers?
Which Key Resources are we acquiring from partners?
Which Key Activities do partners perform?
MOTIVATIONS FOR PARTNERSHIPS:
Optimization and economy
Reduction of risk and uncertainty
Acquisition of particular resources and activities
Key Activities
What Key Activities do our Value Propositions require?
Our Distribution Channels?
Customer Relationships?
Revenue streams?
CATEGORIES
Production
Problem Solving
Platform/Network
Value Propositions
What value do we deliver to the customer?
Which one of our customer's problems are we helping to solve?
What bundles of products and services are we offering to each Customer Segment?
Which customer needs are we satisfying?
CHARACTERISTICS
Newness
Performance
Customization
"Getting the Job Done"
Design
Brand/Status
Price
Cost Reduction
Risk Reduction
Accessibility
Convenience/Usability
Customer Relationships
What type of relationship does each of our Customer Segments expect us to establish and maintain with them?
Which ones have we established?
How are they integrated with the rest of our business model?
How costly are they?
EXAMPLES
Personal assistance
Dedicated Personal Assistance
Self-Service
Automated Services
Communities
Co-creation
Customer Segments
For whom are we creating value?
Who are our most important customers?
Mass Market
Niche Market
Segmented
Diversified
Multi-sided Platform
Key Resources
What Key Resources do our Value Propositions require?
Our Distribution Channels? Customer Relationships?
Revenue Streams?
TYPES OF RESOURCES
Physical
Intellectual (brand patents, copyrights, data)
Human
Financial
Channels
Through which Channels do our Customer Segments want to be reached?
How are we reaching them now?
How are our Channels integrated?
Which ones work best?
Which ones are most cost-efficient?
How are we integrating them with customer routines?
CHANNEL PHASES:
1. Awareness
How do we raise awareness about our company's products and services?
2. Evaluation
How do we help customers evaluate our organization's Value Proposition?
3. Purchase
How do we allow customers to purchase specific products and services?
4. Delivery
How do we deliver a Value Proposition to customers?
5. After sales
How do we provide post-purchase customer support?
Cost Structure
What are the most important costs inherent in our business model?
Which Key Resources are most expensive?
Which Key Activities are most expensive?
IS YOUR BUSINESS MORE:
Cost Driven (leanest cost structure, low price value proposition, maximum automation, extensive outsourcing)
Value Driven (focused on value creation, premium value proposition)
SAMPLE CHARACTERISTICS:
Fixed Costs (salaries, rents, utilities)
Variable costs
Economies of scale
Economies of scope
Revenue Streams
For what value are our customers really willing to pay?
For what do they currently pay?
How are they currently paying?
How would they prefer to pay?
How much does each Revenue Stream contribute to overall revenues?
TYPES:
Asset sale
Usage fee
Subscription Fees
Lending/Renting/Leasing
Licensing
Brokerage fees
Advertising
FIXED PRICING
List Price
Product feature dependent
Customer segment dependent
Volume dependent
DYNAMIC PRICING
Negotiation(bargaining)
Yield Management
Real-time-Market

Figure 4.: Business model canvas (Osterwalder and Pigneur (2010))

2.2.3. Value Proposition Design

The value proposition design is the perfect tool for summarizing all the things that customers want, that the customers do and that customers are afraid of, on one page. This makes it much easier to target the business model exactly to the customer needs. Further, it will create a real value for customers and this will in turn result in a profitable business model. Furthermore, value proposition design provides also the possibility to display all the services/products of a company including how they increase the gain for the customers and how they reduce their pains. The customer profile represents a more deepened definition of the customer segments block from the business model canvas and the value map is a deepening of the value proposition block from the business model canvas. The next step during the value proposition design process is to compare the customer profile, which represents the customer information with the value map, which represents the company information. If the information from the customer profile corresponds with the one from the value map, a so called FIT can be achieved. (Osterwalder et al., 2014)

Customer Profile and Value Map

A customer profile shows the tasks that a customer has to do within a specific context, the things he/she fears and what he/she is looking forward to in this context. For this reason, the customer profile is separated into the following three parts and looks like it is displayed in figure 5 (Osterwalder et al., 2014):

- Customer jobs: These are the tasks that an end-user has to do every day at work.
- Pains: These are the things that an end-user is afraid of.
- Gains: These are the things an end-user looks forward to.

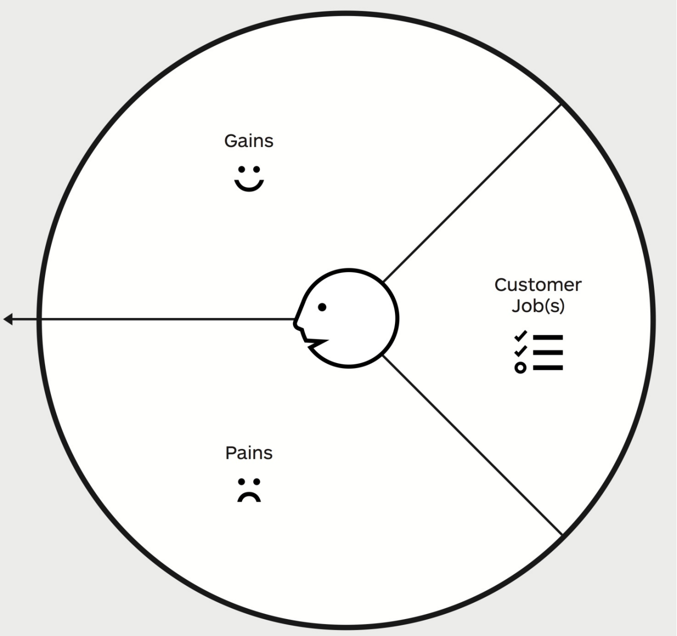

Figure 5.: Customer profile (Osterwalder et al. (2014))

A value map shows everything a company is selling to a customer, the features with which they want to reduce the pains of a customer and the features with which they want to increase the gains of a customer. The value map is, therefore, separated into the following three parts and can be displayed as shown in figure 6 (Osterwalder et al., 2014):

- Products & services: These are the products and services that a company offers.
- Pain relievers: These are the functionalities, that counteract the pains.
- Gain creators: These are the functionalities, that generate gain.

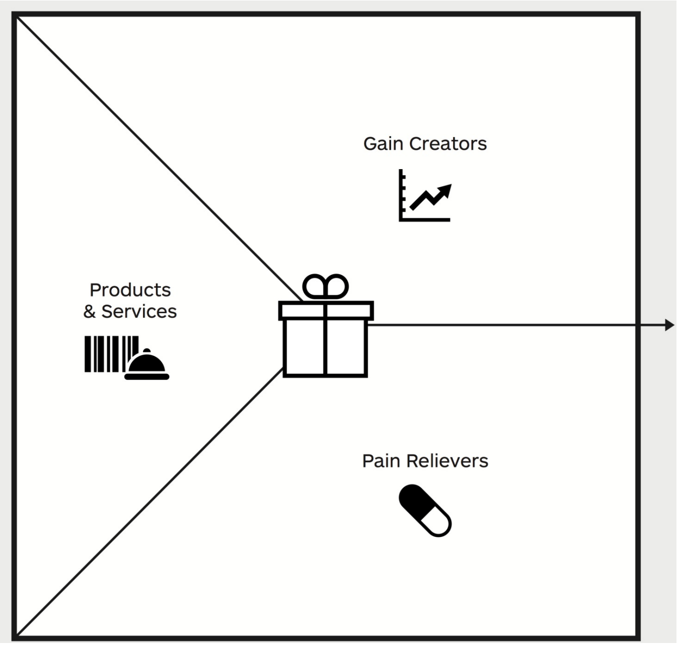

Figure 6.: Value map (Osterwalder et al. (2014))

FIT between Customer Profile and Value Map
A FIT can only be achieved when the value map of the company addresses important jobs, minimizes big pains and creates important gains for the customer. For this reason, the products & services have to fit to the customer jobs, the pain relievers have to fit to the pains and the gain creators have to fit to the gains. No company can address all the jobs, pains and gains and, therefore, it is important to address the most important ones. (Osterwalder et al., 2014)

2.3. Cloud-Based Business Models

An on-premise solution requires the standard licensing model where the licenses relate to a physical machine or to one user. This is not possible for a cloud-based solution, as many users share different resources and therefore usage-based licenses are required. This fact shows that cloud solutions need their own business models. Many companies, therefore, started to establish business models that focus on cloud computing. *Weinhardt et al.*, therefore, define a cloud-based business model framework that provides a hierarchical classification of different business models. This hierarchical classification consists of three layers that are equal to technical layers in cloud realizations. The mentioned cloud business model framework consists of the infrastructure layer, the platform-as-a-service layer and the application layer and is shown in figure 7. (Weinhardt et al., 2009)

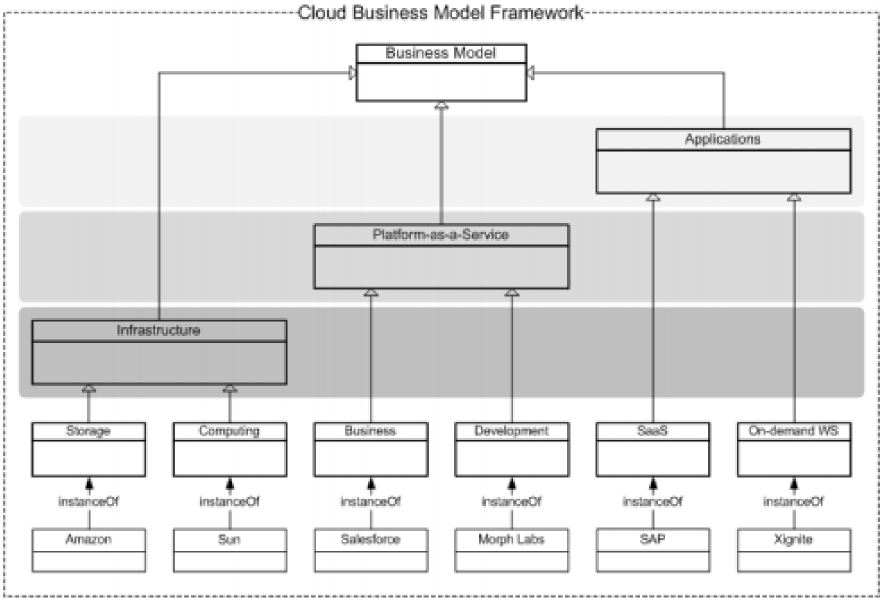

Figure 7.: A cloud business model framework (Weinhardt et al. (2009))

Weiner et al. state that software-as-a-service is a specialized business model. They further mention that software-as-a-service is strictly speaking not a business model but rather a specialized form of software distribution. Nevertheless, if a company offers software-as-a-service it influences the whole business model of the company. The service offer and the benefit for the customer is completely different with an on-demand offer than with an on-premise offer. The customer relationships can be different because of Service-Level-Agreements (SLAs) and other contracts. Many service providers try a vendor-lock-in strategy, which causes a long-term relationship between this service provider and its customers. Furthermore, the provision of the services and the financial model are also different for an on-demand offer compared to a on-premises offer. For these reasons software-as-a-service or on-demand solutions could be seen as an own business model. (Weiner et al., 2010)

2.4. Business Model Environment

The economic landscape is becoming more and more complex and, therefore, it is really important that the environment of the business model is observed continuously. The environment, thereby can be seen as the design space. The design drivers are, for example, new customer needs and design constraints are, for example, regulatory trends. The suggested separation of the environment from Osterwalder and Pigneur (2010) consists of the following four areas: 1) market forces, 2) industry forces, 3) key trends and 4) macroeconomic forces. These four areas are described as follows (Osterwalder and Pigneur, 2010):

1. Market forces: Identify the main market segments and how different issues drive and transform the market. Furthermore, the market needs and how well they are served are an important part of the business model environment. Another important part of the environment are the costs that a customer has when he/she wants to switch to a competitor.

2. Industry forces: Deal with competitors, including their strengths and also with new insurgent companies. Additionally, products that can potentially replace your products, all suppliers as well as other value chain actors belong to the industry forces and have a huge impact on the business model.

3. Key trends: Key trends include technology trends that could threaten or enable your business model to evolve. Furthermore, societal and cultural trends can also influence the business model and need to be identified as well.

4. Macroeconomic forces: In this part of the business model environment the global market conditions (from a macroeconomic perspective) and the capital market conditions are defined.

Another possible separation of the business model environment is proposed by Wirtz (2010). Wirtz (2010) suggests an environmental analysis, that is split in the following areas (Wirtz, 2010):

1. Environment analysis: The environment analysis covers the technological, regulative, economical and the social environment.

2. Industry and market analysis: The industry and market analysis concerns the market structure, the demand-related behavior and the existing industries.

3. Competition analysis: The competition analysis covers the competitive behavior and the intensity of competition.

Knyphausen-Aufseß and Zollenkop (2011) suggest to separate the business model environment into two dimensions. These are the corporate environment and the competition environment and are described as follows (Knyphausen-Aufseß and Zollenkop, 2011):

1. Corporate environment: The corporate environment considers the sociocultural, the ecological, the political-legal, the macroeconomic and the technological aspects.

2. Competition environment: The competition environment examines the industrial relations, the rivalry between the providers, possible new providers, substitution products and the customers and suppliers.

2.5. Legal Basics for Electronic Identification and Transactions

The Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) was published on July 23rd, 2014 and shall apply as of July 1st, 2016. This regulation establishes a framework ensuring that a user's national electronic identification mean issued in one member state is also valid in another EU member state. This electronic identification mean is a so called hard eID, which means that these eIDs are made for identification and authentication at a high assurance level. (Suzic, 2015) Furthermore, electronic signatures and electronic seals shall not be denied as evidence in legal proceedings, just because they are in electronic form or they do not meet the requirements for qualified electronic signatures/seals. Additionally, an interoperability framework will be established to make electronic interactions between businesses, citizens and public authorities from different countries easier. The electronic seal is especially for companies very interesting as they can authenticate all their electronic assets with it. Until now it was always necessary that a natural person, who represented the legal person, signed the electronic assets to guarantee authenticity. For private persons it enhances the comfort, especially when they travel a lot and when they need governmental services from foreign countries. The goal of this regulation is to enhance the trust in electronic transactions throughout the European market and to eliminate obstacles when using electronic identification means across borders. The regulation covers the creation, verification and validation of the following trust services (The European Parliament and the Council of the European Union, 2014):

- electronic identification of natural and legal persons
- electronic signature (as well as advanced and qualified electronic signatures)
- certificate for electronic signatures and seals (as well as qualified certificates for electronic signatures and seals)
- electronic seal (as well as advanced and qualified electronic seals)
- electronic time stamp (as well as qualified electronic time stamp)
- electronic registered delivery services

2.6. Identity Provisioning

Identity provisioning is defined in many different ways through out the literature. These are just a few examples:

Definition 1:
„*Provisioning is the automation of all the steps required to manage (setup, amend & revoke) user or system access and entitlement rights to electronic services.*“ (OASIS Provisioning Services Technical Committee, 2001)

Definition 2:
„*Provisioning is the process of coordinating the creation of user accounts, e-mail authorizations in the form of rules and roles, and other tasks such as provisioning of physical resources associated with enabling new users.*" (Sullivan, 2005)

Definition 3:
„*User account provisioning is a business process for creating and managing access to resources in an information technology (IT) system.*" (Rouse, 2010)

Nevertheless, the definition that suits best for this thesis is the first definition as it is very important that the users of *XiTrust MOXIS* have a valid electronic ID in order to sign documents legally valid. Identity provisioning is very important for the company *XiTrust* as their revenues relate to the number of users who have an electronic ID but it is not only for *XiTrust* very important. Identity provisioning, in general, is getting more and more important as Cloud Service Providers (CSPs) are offering services for many Enterprise Cloud Subscribers (ECS) and ECS are using services from many CSPs. Because of these multi-dependencies, the same identity data of users is stored at different locations, where data consists of different information. Considering these circumstances, creating user accounts is not the big challenge in contrast to the assignment and synchronization of user privileges. (Suzic, 2015)

Identity Provisioning in Austria

Austria was the first country that implemented the Directive 1999/93/EC of the European Parliament and the council on a community framework for electronic signatures. This was done through the federal law on electronic signatures, BGBl. I Nr. 190/1999. (Rundfunk und Telekom Regulierungs-GmbH, 2015) Furthermore, suitable general conditions have been established to realize E-Government through the E-Government law which came into force on the 1st of March 2004 (Digitales, 2015c). Currently 530.000 active mobile phone signatures are in use in Austria (Digitales, 2015b). As more people are applying for an electronic identity, more services are supporting it. Just a few examples of Austrian E-government services are listed below (Digitales, 2015a):

- Applying for study grant.
- Applying for childcare allowance.
- Different services regarding social insurance.
- Different services regarding retirement insurance.
- Electronic delivery (http://www.zustellung.gv.at).
- Tax equalization (https://finanzonline.bmf.gv.at/fon/).

In order to use these services, a person needs to get an electronic identity in Austria. The process of getting such an identity is shown in figure 8 and described in the following paragraphs.
The first step is to visit a certified registration authority. The authorities allowed to do the registration are stated in BGBl. II Nr. 330/2009 §2 (2) (Bundeskanzleramt, 2015).

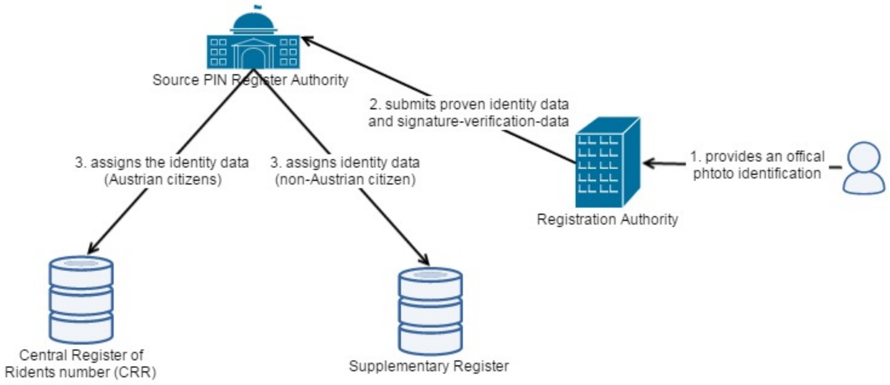

Figure 8.: Registration process in Austria (own illustration)

- The source PIN register authority,
- other authorities on behalf of the source PIN register authority and
- certification service providers which issue qualified certificates on behalf of the source PIN register authority.

When applying for an electronic identity, a person will need to provide an official photo identification. The registration authority then has to submit the proven identity data of the person, together with the used signature-verification-data to the source PIN register authority. This is step two of the figure 8. If the person is an Austrian citizen, the source PIN register authority now needs to check if the submitted data corresponds to the entry of this person in the central register of residents numbers. If the person is a non-Austrian citizen, the source PIN register authority needs to check if the submitted data corresponds to the entry of this person in the supplementary register. This distinction is represented by step three of the figure 8. If the data are matching, the source PIN register authority needs to generate the source PIN and the identity link and send it back to the registration authority, if the registration was not done by the source PIN register authority itself. The identity link mentioned above consists of (Bundeskanzleramt, 2015):

- The name and the date of birth as it is stated in the central register of residents numbers,
- the source PIN and
- the assigned signature-verification-data.

The person now has a valid electronic identity and can use his/her citizen card to provide a qualified electronic signature or to authenticate himself/herself at electronic services for which a qualified certificate is needed. If the person prefers to use his/her mobile phone instead, the same services possible with the citizen card can now be activated via a mobile phone. For a login process with the card, a card reader is needed which is connected to the user's computer. After inserting the card, a PIN has to be entered and authentication is completed. One big advantage of the mobile phone solution is that no card and no card reader are needed. The user just has to enter his/her phone number and a PIN and after a few seconds a text message with a code will be received on the phone. The last step of the authentication process is now to enter this code on the website which the user wants to log in to. (Digitales, 2014) With the card solution, the citizen identification data is stored on the card itself whereby this solution belongs to the user-centric identity model. An advantage of this model is that the user data is stored in his/her domain being fully aware of which data is stored and to whom the data is sent. The solution with the mobile phone, however, stores the identity link at the identity provider, represented by the company A-Trust GmbH in Austria. Thus, this solution belongs to the central identity model, meaning that the identity link will be sent from the identity provider to the service provider and the user is not aware of which data is stored and to whom the data is sent. (Slamanig et al., 2014) If a person wants to change or delete his/her electronic identity, he/she needs to visit the registration authority again.

3. Analysis of Existing Approaches for Services in the Cloud

In the following chapter, different projects and companies dealing with signatures services, identity management and eHealth data in the cloud are described. First of all, a project from Germany called *SkiDentity*. That is about identity management and missing standards and business models in this area. Afterwards, three EU projects are described. The first one, named *epSOS*, focused on cross-border interoperability between eHealth systems and the second, called *EXPAND*, took the results from projects, like *epSOS*, in order to make it more secure. The last EU project focused on identity management in a pan-European context and is called *STORK*. Furthermore, also three companies have been investigated whereby one is rather small and the other two are quite big. The small one is named *PrimeSign* and sells web based signature solutions. The second company provides their customers with electronic identities that are legally valid and the last one deals with electronic signatures and is named *DocuSign*.

3.1. SkIDentity

Cloud computing is a growing area and as identity management is essential in a trustworthy cloud computing environment, the project *SkIDentity* tried to address a secure identity management in the cloud context. Thus, they focused, among other things, on missing standards for eIDs in the cloud, missing business models for identity services in the cloud and unresolved legal issues regarding this topic. In order to solve these problems, they suggested an system architecture as shown in figure 9. The client side shall be realized with the application *AusweisApp* from the German Confederation. In order to integrate cloud services into the SkIDentity-architecture, a cloud connector is provided, which is connected to the client on one side. On the other side, this cloud connector consists of a simple interface which makes it easy to integrate the connector into any cloud or web application. The eID-Broker, the third component of this architecture which is very important, bundles different eID-services so that there exists only one simple interface for authenticating at a cloud service. In order to implement this with the new German identity card, strict standards of the law, regarding identity cards, need to be followed. For using the information from the new German identity card, an authorization certificate is needed. This certificate will be displayed at the client so that the user can see which authority is responsible and for what purpose the data is used. If the user agrees with that, he/she can enter his/her PIN at this point. One restriction causes problems saying that the authorization certificate can not be granted if the reason of the data collection is only to read and to provide the personal data for the card holder or any other person. Strictly speaking, the usage of a broker is not allowed. Therefore, the challenge of the *SkiDentity* project was to develop an acceptable model for using the new German identity card in the cloud. The eID-services together with the identity card are doing the authentication. (Hühnlein et al., 2011)

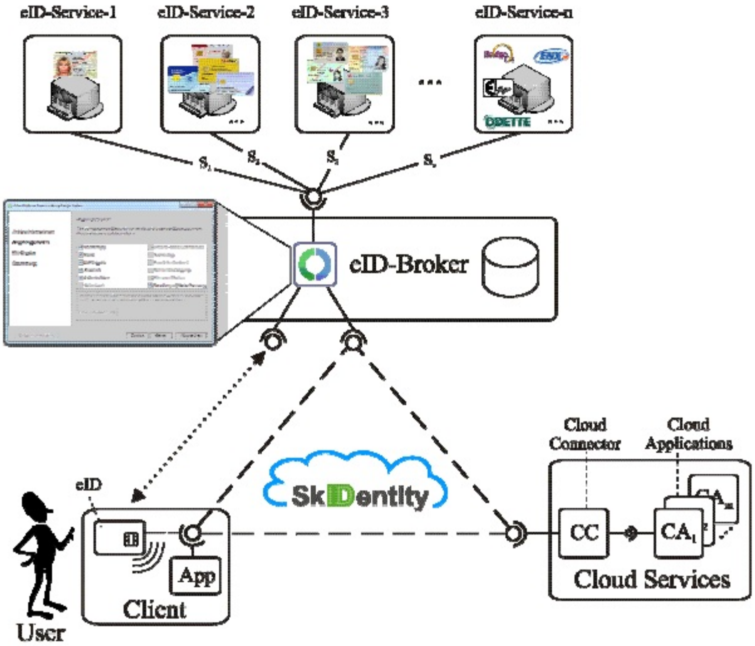

Figure 9.: SkIDentity (Hühnlein et al. (2011))

3.2. epSOS and EXPAND

The project *epSOS - Smart Open Services for European Patients* was a pilot project of the European commission which started in the year 2008 and ended 2014. The goal was to establish a pan-European service infrastructure to facilitate cross-border interoperability between the eHealth systems of different countries. Moreover, accessing patient health information from a different country was made possible and so the quality, especially for persons who travel a lot or live abroad, has been increased. In the first project phase, a patient summary and an ePrescription for a cross-border use was made available. Whereby, a patient summary does not contain the complete history of this patient. It rather consists of some essential information which is good to know when health professionals need it. In order to exchange the patient information with other countries, the *epSOS* project defined *National Contact Points (NCPs)*. *NCPs* are entities that are an interface between the national functions of the national IT infrastructures and those of the European infrastructure. Further, services were defined, tested and evaluated from the patient's and health professional's perspective. *epSOS* also recommended, that the legal conditions that they introduced must be extended to get a sustainable legal framework. Furthermore, they provided their data collection of the patient summaries and worked on semantic sustainability regarding ePrescriptions. (Linden, F., 2008)

Another project which is funded by the European Union is the project *EXPAND*. This project wants to secure services from different pilots and also the services from the epSOS project in order to develop an environment of sustainable cross border eHelath services throughout Europe. Therefore, they want to maintain and expand the services which are already available in terms of interoperability in a pan-European context. Furthermore, they want to bring together stakeholders with knowledge in the development, implementation, assessment, maintenance, dissemination and use of the elements of an EU wide infrastructure. *EXPAND* started in January 2014 and the expected end date is December 2015. (Martins, H., 2014)

3.3. STORK

STORK stands for *Secure idenTity acrOss boRders linKed* and the goal of this project is to establish a single European electronic identification and authentication area. This should be accomplished by allowing people to use their national electronic IDs for electronic services in foreign countries. With four pilots in the areas of eLearning and Academic Qualifications, eBanking, Public Service for Business and eHealth, the *STORK* platform wanted to show the advantages of a borderless digital living. The *STORK 2.0* consortium consists of 19 EU member states / associated countries and tries to establish a common, extensive and long-term vision of eID in Europe.
The eHealth pilot realized that citizen can authenticate themselves with their national ID in a foreign country and access their electronic health records. Moreover, not just the patient can access his/her data, also third parties like family members and health care professionals can do that after they have authenticated themselves with their eID. Additionally, it is possible that health care professionals can authenticate themselves by providing attributes which indicate the profession of this health care professional. (Atos Spain, 2008)

3.4. PrimeSign

PrimeSign is a web based signature solution for signing documents, digitally and legally valid. A signature can be made with the mobile phone, Austrian citizen card, or with any other signature card from any other country but no matter which medium is used, the electronic signature is legally equal to the handwritten signature. Furthermore, countersigning a document or automatically signing a document is also possible, which covers all common signature cases in a company. The signatures and also the according electronic identities from *PrimeSign* are legally valid throughout Europe. In order to ensure that the signing person is really the person he/she pretends to be, *PrimeSign* offers the possibility to identify and authenticate people. Besides that, *PrimeSign* provides different kinds of processes, so that documents can be processed between different departments or even companies without media disruption. Additionally, documents can also be securely edited. One example for this would be their signature file. (Roessler, 2012)

3.5. OPENTRUST

OPENTRUST is an international trust service provider and an international recognized Certificate Authority with partners in more than 20 countries. Furthermore, *OPENTRUST* is the leading company in Europe within the area of protecting customer identities. The services from *OPENTRUST* range from protecting identities and devices to securing electronic documents and transactions. *OPENTRUST* offers its customers electronic passports, ID cards and corporate badges for digitally signing documents and exchanging data securely. The company *OPENTRUST* was founded 10 years ago and is now a market leader in the areas of secure file transfer, electronic signatures and PKI. *OPENTRUST* already has a huge customer base. 50 million people are using *OPENTRUST* to digitally sign their documents every year and 30 million people per day are able to travel safely with the solutions from *OPENTRUST*. (Heritier, 2014)

3.6. DocuSign

The Digital Transaction Management (DTM) platform from *DocuSign* enables companies to keep their transactions digital the whole time. This increases the customer experience as everything goes faster and also saves a lot of money. *DocuSign* was founded in 2003 and has already gained 50 million users since then. Their customer base includes 100.000 customers in 188 countries and therefore *DocuSign* has become a global standard for managing digital transactions. The DTM platform from *DocuSign* enables their customers to sign legally compliant and as their platform is a global standard, they offer their services in 43 languages. The Digital Transaction Management platform manages digital, document-based transactions and established thereby a new category of cloud services. The DTM platform can be integrated into other digital systems such as CRM, HRM and ERP systems. Furthermore, the platform can be used on mobile devices and all the data is also encrypted. (Krach, 2003)

Part II.

Practical Implementation

4. Structure and Approach of the Practical Part

The chapters in this part II, called *Practical Implementation*, describe the results of the measures that have been taken. Therefore, this chapter describes the process that has been established in order to reach the goals, which have been set at the beginning of this master thesis.

4.1. The Approach

The first measure that has been taken, was a general literature review. During this literature review, books and articles regarding business models and value proposition design have been read and general information regarding the state-of-the-art of cloud computing has been collected. (see part I of the thesis)
In a next step, four persons for expert interviews were sought. The requirements for the interviewees were that they are interested in technologies like electronic signatures, cloud computing and that they are already customers of the company *XiTrust* or are interested in becoming a customer. After the interviews, the answers were transcribed and summarized.
Another aspect that became relevant during the literature review and the expert interviews was the legal aspect. In particular the eIDAS regulation as it will come into force on the 1st of July, 2016. It regulates all topics concerning electronic signatures in a European context.
The results of the interviews had also a huge impact on the customer profiles that were set up next. Five customer profiles, whereby, each of them represents a group of people that will get in contact with *XiTrust MOXIS*, have been created. Two of them, the decision maker and the end-user, relate to the general business model and the patient, doctor and hospital administration, relate to the eHealth domain business model. After the creation of the customer profiles, a value map has been created for each of them as well. Afterwards, the value map and the customer profile for each group of people has been compared and checked if they fit to each other. These value maps and customer profiles have been taken and were added to the corresponding business model. The customer profiles to the customer segments block and the value maps to the value proposition block.
The customer profiles and value maps were the starting point for the development of the business models. The information that has been used to develop the business models was gained from

the literature review, the expert interviews and different talks with employees from *XiTrust*. The creation process of the business models, together with the value maps and customer profiles, was an iterative process as more and more details have been obtained over time.
Additionally, the environment of the business model has been defined as suggested by *Osterwalder and Pigneur*. The information for the environment description was mainly gathered through talks with the CEO of *XiTrust*. In order to get also a complete picture of the services that *XiTrust* offers, a service lifecycle map has been developed. The information for this service lifecycle map was gathered through different talks with *XiTrust* employees.
All the requirements that have been gathered throughout the whole process were then collected, sorted, categorized and written down in the master thesis. Furthermore, measures that need to be taken and milestones that should be reached have been defined as well.

4.2. The Structure

Chapter five starts with the description of the approach for the expert interviews and requirements. After that, a short summary of the organizational requirements is given and then the requirements are listed under the different categories. This is the same for the technical requirements and the legal requirements.

Chapter six covers the evolution of the business model and, therefore, starts with the results of the expert interviews. In a next step, the approach for the development of the value maps, customer profiles, business models and the service lifecycle map is defined. Afterwards, the completed value map and the customer profile for the end-users are provided. The next sub chapter defines then the business model environment, followed by the most important part of this chapter, which presents the general business model for *XiTrust MOXIS* in the cloud and the eHealth domain business model for *XiTrust MOXIS* in the cloud. Last but not least, all four phases of the service lifecycle map are presented.

Chapter seven describes all the measures that need to be taken to provide *XiTrust MOXIS* in the cloud. The measures are, thereby, divided into different categories. Thereafter, the milestones are presented and divided into the same categories as the measures before.

Chapter eight provides a short summary and a look ahead.

5. Requirements for a Signature Solution in the Cloud

This chapter starts with the approach for the expert interviews and requirements as shown in figure 10. Further, a summary of all the technical, organizational and legal requirements, that have been collected through an intensive literature review, expert interviews and talks with the employees from *XiTrust*, is provided.

5.1. Approach for the Expert Interviews and Requirements

The whole process from the literature review to the elicited requirements is shown in figure10. The first step as already mentioned before was to conduct an intensive literature review to a gain a better understanding of cloud computing and digital signatures. In order to gain a better understanding of cloud computing and digital signatures, an intensive literature review has been conducted in the chapter 2.

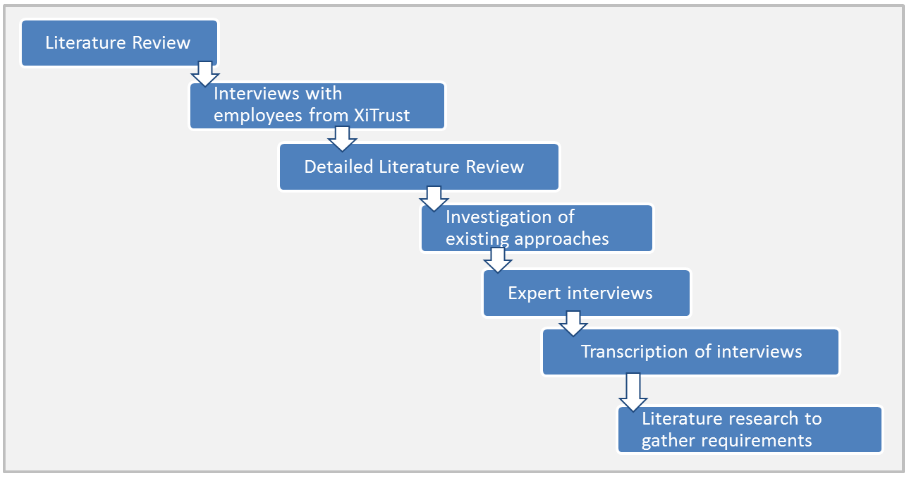
Literature Review
Interviews with employees from XiTrust
Detailed Literature Review
Investigation of existing approaches
Expert interviews
Transcription of interviews
Literature research to gather requirements

Figure 10.: Approach for the expert interviews and requirements (own illustration)

Additionally, a lot of team members from *Xitrust* were asked to explain the different products that they provide and what functionalities their products offer in order to solve their customers problems. After getting a good overview of all the components involved, a more detailed literature review has been carried out. This literature review started with collecting information about identity provisioning, more precisely with a look at how it is done in Austria at the moment. After that, already existing approaches of digital signature services and identity management in the cloud have been investigated.

After some specialist knowledge has been gained, two appointments with two different experts in the areas of digital signatures, electronic identity management and cloud computing have been made. Additionally, also two potential customers of *XiTrust MOXIS* have been interviewed in order to find out what customers expect from a digital signature service in the cloud. One of the experts is a senior developer, working for a university and implementing authentication and signature software. The other expert is the CEO of an IT company, which is developing software to ensure the confidentiality and integrity of documents. From the two customers, one is the head of the IT department of a university and the other one a project manager at a public enterprise.

All the interviews were semi-structured and took approximately 30 minutes. All the interviews started with a general part about the current status of the company regarding document authentication and cloud services. Within the second part of the interview, the interviewee could choose between different use cases for a digital signature service. These use cases have been from two different areas, eHealth and eGoverment. Both uses cases included two smaller cases. The first case of the eHealth use case was about a patient, who goes to the doctor for a routine check-up plus an extensive blood test. The blood test is taken, digitally signed and uploaded to the cloud portal by the nurse. The doctor is now able to see all the data but when the patient visits a dietitian he/she decides to show the dietitian only few values and redacts the rest of the blood test. Figure 11 illustrates this case. The second eHealth case was about a patient, who had tracked all his/her sports activities with a phone/wearable device. After collecting a lot of data, the patient wants to share only the progress with his/her trainer. This case is illustrated in figure 12. The first eGoverment case was about IT providers who have split up their databases and stored the multiple parts at independent cloud providers. If a data loss happens now, only a predefined subset of the multiple parts are needed in order to restore all the data. The second eGoverment case considered a forest fire and the government would want to publish a report about this incident. This report should include victims, rescue workers and so on but should not include personal information about them such as names. The last part of the interview was about the requirements of a digital signature service in the cloud and also about expectations and concerns of such services. All the interviews have been recorded and notes were taken as well.

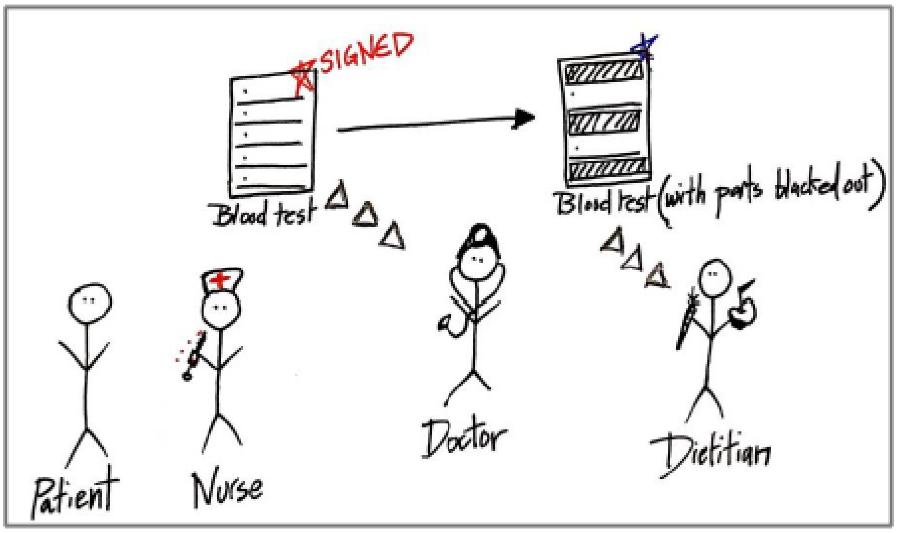

Figure 11.: Blood test case (Alaqra et al. (2015))

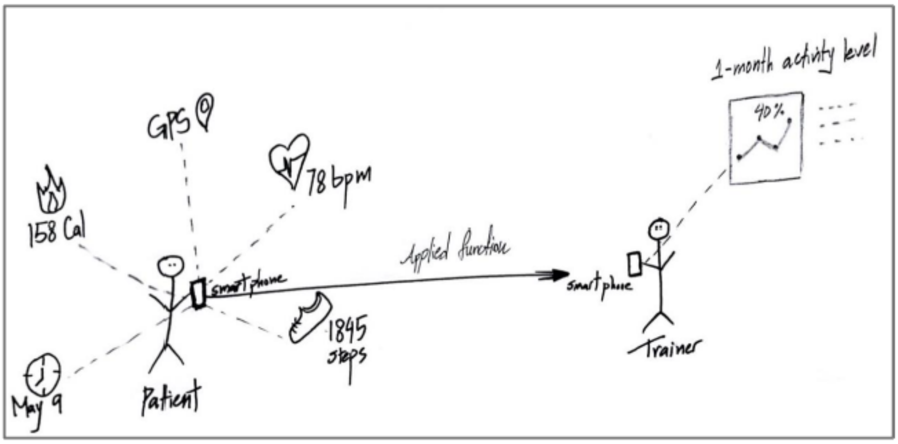

Figure 12.: Tracking device case (Alaqra et al. (2015))

The next step was then to transcribe the interviews. The result from the transcription and the hand written notes were then summarized in this thesis (see chapter 6). Subsequently, an exhaustive literature research was started to gather all technical, legal and organizational requirements for providing a signature service in the cloud.

5.2. Organizational Requirements

This section lists all the organizational requirements that have been elicited during the literature research, the expert interviews and also during the talks with different *XiTrust* employees. The organizational requirements in this case cover all the activities that *XiTrust* needs to arrange and install in order to provide *XiTrust MOXIS* in the cloud. The requirements in the following are structured in a way that first of all, general measures that *XiTrust* needs to be taken are described. After that, the section *Standards and Principles* presents all the standards that need to be fulfilled. The next requirements affect the customer needs and wishes, followed by some rules from the cryptography field that need to be considered. Thereafter, some requirements regarding the obligations of administrators are described. Last but not least, actions that should take place concerning incidents and the recovery of them as well as a backup strategy are described. All these requirements are classified into three different importance levels. These levels are named *MAY*, *SHOULD* and *MUST*. *MAY* are the least important requirements and *MUST* are the most important requirements.

5.2.1. General Measures XiTrust has to take

The first section of the organizational requirements defines that *XiTrust* needs to be very transparent regarding how they act and what they provide. It also describes that they need to check their service if it works properly and secure but they also need to check if their subcontractors work correctly. Furthermore, the data of the users need to be held secure by *XiTrust* and also when data is send to other subcontractors. Data safety, during the time when the customers use the signature service, is not enough. Exit scenarios and what happens with the data in case of an exit scenario, is regulated in the following requirements. These requirements are listed in table 1.

Requirements	**Importance**
The service provider needs to do the billing in a way so that it is understandable for the customer. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST
The information held for the customers as well as the information about the customers need to be protected and security breaches need to be reported immediately. (Reed et al., 2011)	MUST
XiTrust needs to check the companies *Raiffeisen* and *A-Trust* regarding security or request evidence of their security checks. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST
Code Reviews, automatic review tools and vulnerability tests need be used and performed. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST
General as well as quantitative service descriptions need to be defined in SLA's. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST
An enterprise risk management needs to be established including the services and also the provider's subcontractors (e.g.business survivability of subcontractors). (Reed et al., 2011)	MUST

Requirements	Importance
The time when all data from all storages has to be deleted after a customer left needs to be defined. (Interview)	MUST
Customers all over Europe must have a valid electronic identity. (Interview)	MUST
Some people all over Europe need to be educated as registration officers. (Interview)	MUST
The amount of resources used needs to be monitored, controlled and reported so that all parties involved know, how much the services have been used. (Interview)	MUST
A service catalog that describes the offered services needs to be provided.(Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD
A consistent branding is needed to ensure trust. (Interview)	SHOULD
The code of conduct needs to be displayed on the website as risks and incentives need to be clear in the health sector. (Alaqra et al., 2015)	SHOULD
The trustworthiness of *XiTrust* and the subcontractors needs to be verified by an independent body. (Alaqra et al., 2015)	SHOULD
Practical privacy policies are needed in order to inform the end user about the location of the cloud server and the jurisdictions that will apply. (Alaqra et al., 2015)	SHOULD
Tools that check cloud services and delete data after their retention period expired are needed. (Alaqra et al., 2015)	SHOULD
An exit strategy is needed in case of a normal termination (expiration of the service agreement) or an unexpected termination (service provider goes bankrupt). (Jansen et al., 2011)	SHOULD
An effective procedure is needed to delete data including previous versions, temporary data and also data fragments. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD
SAML, WS-Federation (an identity federation specification) or SSO via VPN should be used for identity federation and identity attribute exchange. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD
The least privilege model should be applied for every user (admin, customer,...). (Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD
Cloud services should be monitored 24/7. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD
An independent organization should audit *XiTrust, Raiffeisen* and *A-Trust*. (Reed et al., 2011)	SHOULD
Tutorials for the functions and limitations need to be provided. (Alaqra et al., 2015)	SHOULD
New features need to be available immediately to all customers. (Interview)	SHOULD

Requirements	**Importance**
XiTrust needs to provide information how data can be protected in an easy way. (Horvath and Agrawal, 2015)	MAY
A cloud access security broker (CASB) is needed for securing cloud data between the cloud and the customer device. (Bitglass, 2014a)	MAY
The risk management performance needs to be measured (with e.g. Security Content Automation Protocol). (Reed et al., 2011)	MAY
XiTrust and all subcontractors need to agree on a common certification assurance framework (e.g. ISO). (Reed et al., 2011)	MAY

Table 1.: General Measures

5.2.2. Standards and Principles

All the requirements regarding principles and standards that should be followed are listed in table 2.

Requirements	**Importance**
All applications should be compliant with the Open Web Application Security Project (OWASP) principles. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD
An Information Security Management System needs to be based on the ISO 27001/2 standard or on the BSI standard 100-2. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MAY
Business Continuity Management needs to be in place and based on standards such as BS 25999 or BSI 100-4. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MAY
All offered services need to be ISO27001 certified. (Lambo, 2012)	MAY
The ISO/IEC 27017 standard should be followed regarding information security of cloud computing. (Reed et al., 2011)	MAY
The ISO/IEC 27036 standard should be followed regarding the evaluation and treatment of information security risks when receiving services from suppliers. (Reed et al., 2011)	MAY

Table 2.: Standards and principles

5.2.3. Customer Needs and Desires

The requirements in this section deal with the wishes of the customers. The requirements define what customers want to be able to do and what *XiTrust* or rather their service *XiTrust MOXIS* needs to provide to satisfy the customer. All these requirements are displayed in table 3.

Requirements	**Importance**
Customers want to know where and how their data is stored. (Horvath and Agrawal, 2015)	MUST
The customer has the exclusive ownership of all the data that belongs to him/her. (Reed et al., 2011)	MUST
Customers need to be able to monitor the performance of the used services. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD
The customers need to be informed of the subcontractors, *A-Trust* and *Raiffeisen*. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD
The customers need to be informed of where their data is stored and where their data is processed to. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD
Transparency regarding what *XiTrust, Raiffeisen* and *A-Trust* do with the data from the customers is required. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD
Customers want to control, how their data is used. (Horvath and Agrawal, 2015)	MAY
Customers want to learn about the provider's products, data safety and want to be trained in that area. (Horvath and Agrawal, 2015)	MAY
The benefits as well as the risks and limitations of cloud computing need to be explained to the users. (Alaqra et al., 2015)	MAY
A service with which the customer can test the security of the whole cloud environment is needed (e.g. CloudInspect). (Markey, 2011)	MAY
The customers should have the right to audit *XiTrust* and their subcontractors. (Reed et al., 2011)	MAY

Table 3.: Customer needs and desires

5.2.4. Cryptography

The requirements in table 4, deal with organizational measures that need to be taken in the cryptography sector.

Requirements	**Importance**
Cryptographic keys should only be used for one intended purpose. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST
The keys for encrypting the signed documents always need to be stored encrypted, redundant and the keys need to be recoverable. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST
The keys for the signed document encryption need to be distributed securely. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST
The keys for encrypting the signed documents need to be exchanged regularly. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST
In order to access the key administration function, a separate authentication is needed. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST
The keys that are no longer required need to be deleted securely. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST

Table 4.: Cryptography

5.2.5. Administrators and their Duties

This section defines the requirements an administrator needs to fulfill in order to guarantee a secure cloud service. These requirements are listed in table 5.

Requirements	**Importance**
Administrators are not allowed to have keys from customers. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST
Administrators need to authenticate themselves with a two-factor authentication. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD
Network accesses and IT-resource accesses from the employees of *XiTrust* should be secured with a two-factor authentication. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD
All actions of the administrators need to be logged. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD

Table 5.: Administrators and their duties

5.2.6. Incidents and Recovery

The actions that need to be taken if an incident occurs or the actions to prevent an incident are collected in table 6. Additionally, also measures to recover from such incidents are provided.

Requirements	**Importance**
Services to mitigate DDoS attacks need to be in place for internal attacks (one cloud user attacks other cloud users) and external attacks. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST
An anti-virus software is needed so that no harmful documents can be uploaded. (Interview)	MUST
An incident response plan needs to include, how incidents can be detected and handled. (Reed et al., 2011)	SHOULD
An incident reporting tool is needed to inform end users about incidents. (Alaqra et al., 2015)	SHOULD
Incidents shall be detectable and explainable. (Alaqra et al., 2015)	SHOULD
Data protection concerns, disaster recovery plan for a network failure and also how the data, which is stored by a subcontractor, can be accessed if the subcontractor goes bankrupt need to be considered. (Eriksdotter, 2010)	SHOULD
A plan for how attacks can be detected need to be created with a special focus on internal attacks (one cloud user attacks another cloud user). (Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD
Security measures should be checked regularly. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD
Results from the security checks should be published in a suitable way. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD
Incident handling for each stage of the incident handling process (from detecting an incident to the recovery) must be defined in the SLA's. (Reed et al., 2011)	MAY
The incident response plan should be checked by the customers and *XiTrust* at least once a year.	MAY
(Reed et al., 2011) All business processes and services need a prioritization for the recovery. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MAY
The platform *CloudeAssurance* could be used for rating risks and monitoring systems. (Lambo, 2012)	MAY

Table 6.: Incidents and recovery

5.2.7. Backups

This section deals with backups, starting from a backup structure that is needed up to a procedure for recovering those backups. These requirements are defined in table 7.

Requirements	**Importance**
Data backups need to be made and checked whether they work or not. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST
A secure backup structure is needed because backups might be the target of attacks. (Alaqra et al., 2015)	MUST
Backups should be made automatically and regularly. (Alaqra et al., 2015)	SHOULD
Backups need to be encrypted. (Alaqra et al., 2015)	SHOULD
A procedure for recovering the backups needs to be defined. (Alaqra et al., 2015)	SHOULD
Backup services shall be available all the time. (Alaqra et al., 2015)	SHOULD

Table 7.: Backups

5.3. Technical Requirements

In the following sections, the technical requirements are split up into four areas. The first area deals with technical requirements regarding the usability of *XiTrust MOXIS*. The second section covers the security requirements, that need to be fulfilled. Thereafter, the requirements that concern the uptime and performance of a cloud service are listed and the last section defines requirements regarding tests and checks that should be made before such a service will be delivered. All these requirements are classified into three different importance levels. These levels are named *MAY*, *SHOULD* and *MUST*. *MAY* are the least important requirements and *MUST* are the most important requirements.

5.3.1. Usability

The requirements in table 8, define the expected features of the signature service *XiTrust MOXIS* in the cloud regarding usability.

Requirements	Importance
All users should only see the documents that they need for their tasks. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST
The user interface (UI) of the application needs to be suitable and intuitive. (Alaqra et al., 2015)	SHOULD
The service needs to be available in different languages. (Interview)	SHOULD

Table 8.: Usability

5.3.2. Security

This section concerning the security includes requirements for how a network should be separated and the encryption of data. Furthermore it is also defined what security measures could be set up for the user authentication. All these requirements are listed in table 9.

Requirements	**Importance**
The customers need to be separated at all layers on the cloud computing stack (application, server, network, storage, etc.). (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST
All the data sent between *A-Trust, Raiffeisen, XiTrust* and their customers needs to be encrypted. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST
The keys for encrypting the signed documents need to be created in a secure surrounding and a suitable key generator needs to be used. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST
All documents should be stored encrypted and securely. (Interview)	MUST
Strong passwords for the user authentication or even a two-factor authentication is needed. (Interview)	MUST
Every customer needs to get an individual URL in order to reach the service. (Interview)	MUST
The database needs to be multi-client capable. (Interview)	MUST
The network needs to be segmented into different security zones regarding how much protection they need. For example, one for the management of the cloud, one for the storage network, and so on. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD
Data ex- and imports from and to the data center should be documented and checked. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	SHOULD
Policies need to separate the network traffic regarding origin and destination in order to mitigate the risk of unauthorized accesses. (Ayoub, 2013)	SHOULD
The cloud environment (e.g. servers) and the security solution protecting it should be modifiable on demand. (Ayoub, 2013)	SHOULD
The cloud server code should include only the minimum of information that is necessary. (Reed et al., 2011)	SHOULD
An end-to-end encryption needs to be in place and only the user has the ability to decrypt the data. (Interview)	SHOULD
A linkage between the signatory and his/her e-mail address is needed. (Interview)	SHOULD
The user needs to wait a few seconds after several failed login attempts. (Interview)	SHOULD
A SSO solution is needed so that the customer only needs one password for all applications. (Bitglass, 2014b)	MAY

Table 9.: Security

5.3.3. Uptime and Performance

The requirements in table 10 are defined in order to satisfy the customer expectations of a cloud service in terms of uptime and performance. These requirements ensure that the application will run smoothly even though the server, that performs the service runs remotely and has to deal with a huge amount of data.

Requirements	**Importance**
The application needs to run as it would run when it is operated locally regarding reliability, availability, and security. (Liang and Ulander, 2010)	SHOULD
The application should deploy and scale easily. (Bitglass, 2014b)	SHOULD
The application needs to be designed in a way that it needs a minimal bandwidth and delivers a maximal performance so that the application operates efficiently in the cloud. (Commvault, 2015)	SHOULD
The application needs to perform well even if a large data set needs to be transfered. (Alaqra et al., 2015)	SHOULD
XiTrust MOXIS needs to be available 24/7. (Interview)	SHOULD

Table 10.: Uptime and performance

5.3.4. Tests and Checks

The requirements concerning the tests are important in order to guarantee a stable software. For this reason, the requirements in table 11, define that checks regarding programming errors, tests with all possible inputs and also interoperability tests need to be made.

Requirements	**Importance**
Checks regarding the typical programming errors such as Race Conditions or Buffer Overflows should be made. (Reed et al., 2011)	MUST
Dynamic code analyses, where the code will be tested like it would run in the cloud, should be made. (Reed et al., 2011)	MUST
Interoperability testing is needed in order to detect if the cloud service is able to exchange information with other components or applications. (Reed et al., 2011)	MUST
The services need to be tested with all possible inputs from the user or other systems. (Reed et al., 2011)	SHOULD
Penetration testing is needed to reveal the strengths and weaknesses of cloud service's network security. (Reed et al., 2011)	SHOULD

Table 11.: Tests and checks

5.4. Legal Requirements

Last but not least, the legal requirements define how the licenses should be managed, that contracts are needed between all parties and that data protection directives/laws as well as the eIDAS regulation must be followed. All these requirements are listed in table 12 and are classified into three different importance levels. These levels are named *MAY*, *SHOULD* and *MUST*. *MAY* are the least important requirements and *MUST* are the most important requirements.

Requirements	**Importance**
Software licenses must be usage-based (CPU-hour, user, etc.). (Reese, 2009)	MUST
All parties involved need to sign a contract which defines the needs and obligations throughout the validity of the contract and upon termination. (Reed et al., 2011)	MUST
Data protection directives and data protection laws must be followed. (Bundesamt für Sicherheit in der Informationstechnik, 2012)	MUST
Within Europe, the *eIDAS* regulation applies. (Interview)	MUST
Online terms and conditions need to be easy to understand and need to be short. (Horvath and Agrawal, 2015)	SHOULD
A user-based licensing model can be subdivided into concurrent users and total users. (Foran, 2010)	MAY
Contractual agreements might be needed to specify for which purposes the data is used. (Reed et al., 2011)	MAY

Table 12.: Legal requirements

6. Evolution of a Business Model

In this chapter, the results of the four expert interviews are presented. Thereafter, the business model environment for *XiTrust MOXIS* in the cloud is described with the help of the four different perspectives that are suggested by *Osterwalder and Pigneur*. These four perspectives are the industry forces, the market forces, the key trends and the macro economic forces. Furthermore, one of the completed value maps and customer profiles is presented. The main part of this chapter covers the presentation of the general business model for *XiTrust MOXIS* in the cloud and the eHealth domain business model for *Xitrust MOXIS* in the cloud. Afterwards the service lifecycle map for *XiTrust MOXIS* is described, where all the phases that a customer will go through, when he/she is going to buy or use *XiTrust MOXIS* in the cloud, are described.

6.1. Results from Expert Interviews

In the following section, the results from the expert interviews are presented. The interviews themselves can be found in the appendix and as the interviewees want to stay anonymous these four abbreviations GL, AS, TL and CM represent the interviewees. The interview was separated into 3 parts. The first part affected the current status of companies regarding electronic signatures and cloud services. The topic of the second part were different use cases from the eHealth area and from the eGoverment area and they had to choose one of these use cases. The last part covered questions about the requirements of digital signatures and cloud services.

6.1.1. General Inquiry

An interesting fact that has been found during the general questions at the beginning was that three of the four interviewees already use electronic signatures to authenticate documents and one of them uses them even mainly. This is quite different when it comes to the usage of cloud services because most of them use it only a bit and in a very restricted way. When the interview came to the point of sharing data with people outside the company, the most common answer was to use e-mail and if an authentication is required, a digital signature would be used. Only one person answered that they give the people access to their infrastructure and are even thinking of providing a cloud solution soon.

6.1.2. Health Care Use Case

Figure 13 illustrates this use case very well and this figure was also shown to the two interviewees, who have chosen this use case, during the interview. It is about a patient who records personal data of all his/her activities, with a smart phone/wearable device. In a next step, the patient wants to share this information with a trainer but he/she wants to send only the activity progress information and not all the data. The feedback for realizing such a case was very good. The interviewees said that they would like it, if they know, which information is passed on as it feels better if the recipient of the information is known. Another reason why they liked it was that they think that it is not necessary that the recipient gets all the information.

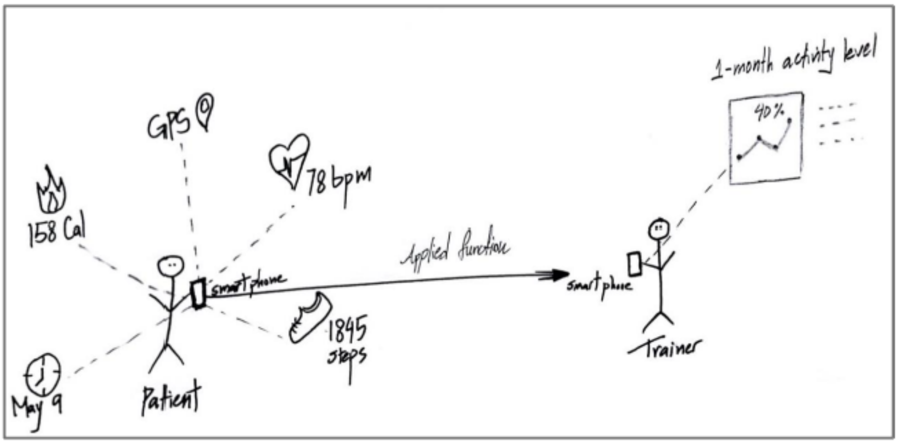

Figure 13.: Health care use case (Alaqra et al. (2015))

6.1.3. E-Government Use Case

This use case is about a forest fire and the government wants to release a report about this incident. This report includes personal information about victims, rescue workers and other sensitive data but before the report gets published, all the personal information such as the names of the rescue workers should get anonymized. The report has been signed before the anonymization happened. The feedback regarding the validity of the signature was diverse. One of the interviewees said, that it is only valid if the person signing the report and the person changing the report are the same. The other interviewee argued that the signature is not valid as the report has been changed after it was signed and therefore the signature is broken. They had also different opinions about blacking out information of a signed document. One said, that it needs to be resigned afterwards and the other said, that it needs a process that can state that the document has been valid before information was blackened. Regarding the existence of such systems in their company, one negated and the other one said, that there would exist a lot of cases and they would really like to have such a system. He said, further, that such a system is not practically realized yet but that they have implemented prototypes of such systems. Their prototypes use blank digital signatures in order to handle modifications and a template is used to guarantee that the modified documents have a valid signature. This template, where every field has two properties, blackened or real value, will be signed before and after fields get blackened. For this reason the validity of the document itself can be validated and all the instances with blackened or not blackened fields can also be validated.

6.1.4. Requirements Follow Up

The focus of the last part of the interview were requirements of signature services in the cloud but also concerns about such services and if contractual agreements would be enough to ensure security or if cryptographic solutions would be preferred. The requirements in this section have been elicited from the interviews and all requirements together are listed in chapter 5.
The answers regarding the requirements of digital signature services in order to be considered trustworthy, secure, private and authentic were very different. One said, that the mobile phone signature fulfills these requirements perfectly, while it was very important for another one that the service operates locally and that it needs to be very clear which data is send outside. Another interviewee provided requirements that need to be considered during the implementation of such a service. He said, that the libraries in use need to be up-to-date, that the programmers need a profound knowledge regarding cryptographic processes and that the certificate authority needs to be trustworthy. Further requirements that have been mentioned were that the service needs to be implemented and maintained correctly regarding security and privacy directives. Additionally, to the compliance with the law also complete transparency is requested. Nevertheless, the interviewees stated that the user needs to trust this system because otherwise the service will never succeed.

The answers regarding requirements for the use of cloud services in their own organization was a bit different. Two simply said, that they do not use cloud services and the other two mentioned that the data needs to be stored securely and complete transparency is required but that they have to trust a third party in the end. They further demanded, that this third party needs to be audited.

When it came to the concerns of such systems, none of the interviewees had technical concerns, it was all about trust and legal issues. One example that the interviewees mentioned, was that the customer needs to get convinced that the cloud service is secure and that it is trustworthy. Another example were legal concerns, regarding where is the information really stored and what can the users do if an incident occurs.

The answers regarding the question, if they trust contractual agreements or cryptographic solutions more, were very clear. All of them said, that they trust cryptographic solutions more and only one added that contractual agreements are also necessary. Their favorite idea was an end-to-end encryption so that the cloud provider has no possibility to get the data.

6.1.5. Results and Impacts of the Interviews

The results from the interviews did not have a direct impact on the business models but they provided good insights about the current status of different companies regarding cloud services and electronic signatures now and also what they can imagine in the future. Even though it did not directly impact the business models, some important requirements could be elicited from the interviews. These requirements are:

- All documents should be stored encrypted and securely.
- An end-to-end encryption needs to be in place and only the user has the ability to decrypt the data.
- Within Europe the *eIDAS* regulation applies.
- Data protection directives and data protection laws must be followed.
- Contractual agreements might be needed to specify for which purposes the data is used.
- Incidents shall be detectable and explainable.
- An incident reporting tool is needed to inform end users about incidents.
- The information held for the customers as well as the information about the customers needs to be protected and security breaches need to be reported immediately.
- Transparency regarding what *XiTrust, Raiffeisen* and *A-Trust* do with the data from the customers.
- The customers need to be informed of where their data is stored, where their data is processed to and how it is stored.
- The customer has the exclusive ownership of all the data that belongs to him/her.
- The trustworthiness of *XiTrust* and the subcontractors needs to be verified by an independent body.
- An independent organization should audit *XiTrust, Raiffeisen* and *A-Trust*.

6.2. Approach for Value Maps, Customer Profiles, Business Models and Service Lifecycle Map

After the interviews have been conducted, the creation of the customer profiles started. In the first iteration, the customer profile was compiled for an average *XiTrust* customer. According to this customer profile, a value map was also created. With this customer profile and value map, a first business model was developed. After the development of a first version of the business model, a workshop was held together with my supervisor from the University of Technology, Graz and my supervisor from the company *XiTrust*.

As the first iteration of the business model was very general, the goal for the next iteration was to split up the business model and also the value map and customer profile. For this reason a business model for the eHealth domain, where the customer segments building block consists only of hospitals, was created. The more general business model has then been changed in a way that only the following three customer segments were left: small, medium and large sized companies. This caused also a separation of the value map and customer profile. Therefore, five value maps and customer profiles, whereby two of them were focusing on the general business model and three were focusing on the eHealth domain business model, were created. The two value maps and customer profiles for the general business model represent on the one hand the end-user and on the other hand the person who makes the decision, if the product/service will be bought or not. The three value maps and customer profiles for the eHealth domain business model represent the patient, the doctor and the hospital administration. After the five customer profiles were created, the five value maps were created as well. Each of the couples was investigated and a check regarding the FIT, as it is mentioned by Osterwalder et al. (2014), was made. Besides the iterations of the business model, the customer profiles and value maps, a service lifecycle map was created iteratively as well. The starting point of each iteration was the information phase, followed by the offer and purchase phase, the order and execution phase and the use phase of the service lifecycle map. This whole process is illustrated in figure 14.

6.3. Customer Profile and Value Map for the End-Users

In this section the customer profile and the value map for the end-users of the general business model are described. End-users in this case represent those people in a company who need to sign a lot of documents and not private persons. The other value maps and customer profiles can be found in the appendix A as they are just slightly different than this one. The value maps and customer profiles have been made, to organize what the customer wants in one figure and to display how value can be created for the customers. Furthermore, the customer profile and the value map make it easier to target the business model exactly to the needs of the end-users.

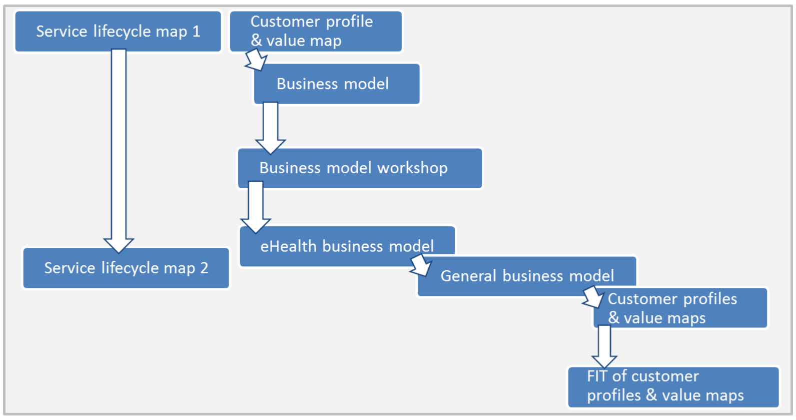

Figure 14.: Approach for value maps, customer profiles, business model and service lifecycle map (own illustration)

6.3.1. Customer Profile for the End-Users

All the jobs, gains and pains from the customer profile of the end-users have a focus on *XiTrust MOXIS* in the cloud and the numbers show how important they are for the end-users. The ranking starts with 100, meaning it is very important and ends with 0, which means that it is not important at all. According to the expert interviews and the conversations that have been held with different *XiTrust* employees, the following customer jobs, pains and gains have been identified for the end-users and are presented in figure 15.

Jobs of the End-Users

First of all, an end-user needs to **sign documents** and most *XiTrust* customers need to sign a lot of documents so this is quite a big part of the customers work. Additionally, a lot of end-users also need to **gather many signatures from different people** throughout a company, so this is also very important for them. One job that is even more important for them when they heard from a signature service in the cloud was to **protect their personal information**. Besides that, also some general jobs have been identified. The two most important ones are that they need to **do their daily work** and that they have to **appear competent**. The job least-important for the end-users is to **make decisions**.

Pains of the End-Users

The biggest pain for the end-users would be that their **personal data gets lost or abused**, when they use a signature service in the cloud. The second pain, that got the highest rating, is that they would **fail in their job**. A pain that is quite similar to that one is that the end-users are **not able to use the new platform** because they do not have the right skills to use it. The problem that the **service simply does not work** from time to time also has the second highest rating. Another pain for them would be that they **miss a deadline** because the service is down and it would also be a pain for them, if they **do not know who will receive their data**. A pain that relates to the pain before is that the service is **not trustworthy**, which means that people, who should not get access to the information, get access. The next pain that has also been rated as quite important is that end-users **do not get help when they have a problem** with the service. Some potential customers also said that it would really be a pain, if the **service is faulty** and does not work as expected. Furthermore they also said that another pain would be, if the service is **not easy to use**. Everyone has a lot of passwords to remember by now so it is understandable that it would be a pain for the end-users if they have **another password to remember** for this service. Something end-users are also afraid of is that their signature with *XiTrust MOXIS* in the cloud is **not equal to the handwritten signature**. Another pain that the end-users mentioned is that they always need to have a **network connection** if they want to sign a document. Not a huge pain, but a bit annoying for customers, is the fact that each end-user **needs to get a hard eID** before he/she can make a qualified electronic signature.

Gains of the End-Users

The biggest gain for the end-users would be if they can **sign fast and straightforward**. A gain that was also rated really high was to **sign everywhere**, so that they do not need to come to the office for example just for signing a few documents. Another gain would be to **sign any time** which would be very convenient for the end-users because they could just sign the documents when they have time. The next gain that also got the second highest rating is, **getting signatures from others faster** because if a lot of people need to sign a document one after the other, it takes a lot of time and the people need to be in the office at the right time. Another gain with a high rating, is the gain that it should be **more convenient** so that they can, for example, sign many documents by just going through the signing process once. A big gain for the end-users would also be **good usability** of the signature service, meaning that the graphical user interface should be very intuitive and every task should be easy to find. Another gain would be to **get support** whenever they need it. Further, they would appreciate it, if they **get all their work done in time** as they can save time with the new service. A consequence of this would be that they can **go home early**, which is another gain for the end-users. One pain of handwritten signatures is that you cannot see if somebody forged the signature and, therefore, the end-users would benefit from **verification tools** for signature validation. Another gain would be if the service is **self-explanatory** so that they do not need a training and they do not need to read the handbook every single time they use the service. One gain for the end-users would also be if they could **impress the boss** by using the new service so efficiently that they have more time for other tasks. The end-users see it also as a gain if they could **work with new technologies**.

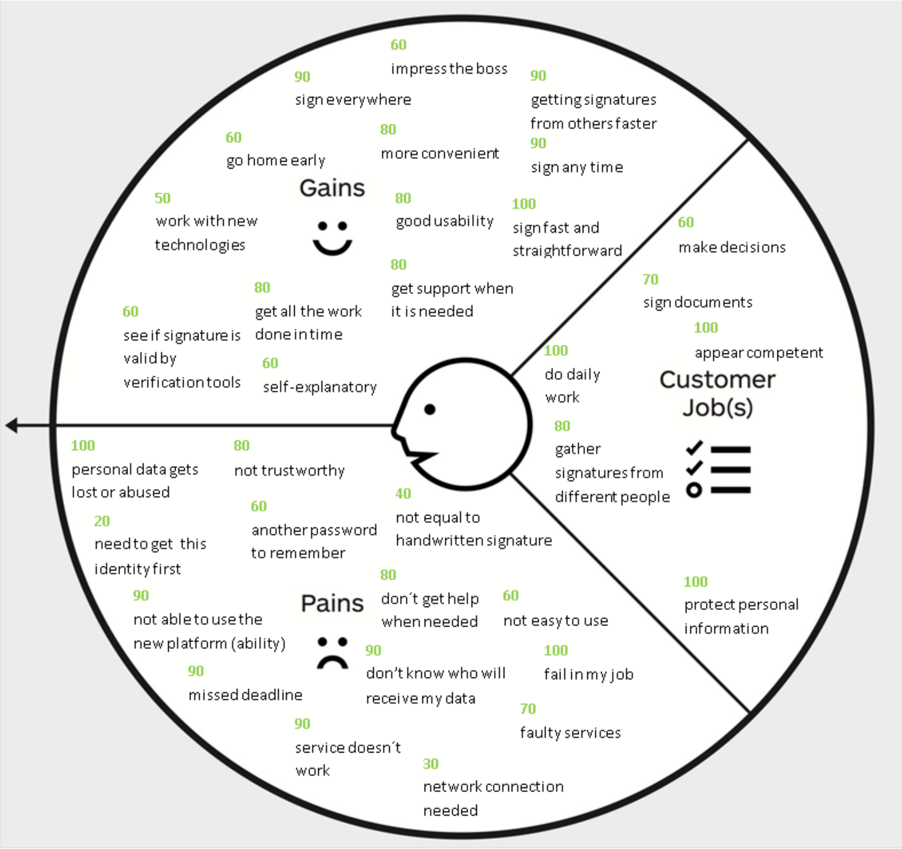
60
impress the boss
90
sign everywhere
90
getting signatures from others faster
60
go home early
80
more convenient
90
sign any time
Gains
50
work with new technologies
80
good usability
100
sign fast and straightforward
60
make decisions
80
get support when it is needed
80
get all the work done in time
60
see if signature is valid by verification tools
70
sign documents
100
appear competent
60
self-explanatory
100
do daily work
Customer Job(s)
80
gather signatures from different people
100
personal data gets lost or abused
80
not trustworthy
60
another password to remember
40
not equal to handwritten signature
20
need to get this identity first
80
don´t get help when needed
60
not easy to use
100
protect personal information
Pains
90
not able to use the new platform (ability)
90
don't know who will receive my data
100
fail in my job
90
missed deadline
70
faulty services
90
service doesn´t work
30
network connection needed

Figure 15.: The customer profile for the end-users (own illustration based on Osterwalder et al. (2014))

6.3.2. Value Map for the End-Users

All the products & services, pain relievers and gain creators have a focus on *XiTrust MOXIS* in the cloud and the numbers show how important they are for the end-users. The ranking starts again with 100, meaning it is very important and ends with 0, which means that this is not important at all.The following products & services, gain creators and pain relievers for the value map of the end-users were also gained trough different talks with the *XiTrust* employees and by reading different handbooks and are presented in figure 16.

Products and Services for the End-Users
The most important product in order to provide *XiTrust MOXIS* in the cloud, is ***XiTrust MOXIS***. *XiTrust MOXIS* enables the user to **digitally sign documents** in a way that the signature is legally equal to the handwritten signature and the **documents can be encrypted and decrypted** as well. For this reason, these two services are linked with an arrow to *XiTrust MOXIS*, as shown in figure 16. The next service that *XiTrust* offers is **support from 9 a.m. to 5 p.m.** so that the end-users can call and ask for help if they have any problem with their products. Another service that

XiTrust offers is that they can **integrate *XiTrust MOXIS* in the workflow system** in a way that the end-users do not even recognize the system change. Before a person can use *XiTrust MOXIS* he/she needs a hard eID and those hard eIDs can be issued by an registration officer (RO). Therefore, *XiTrust* offers the **training of ROs** for one or two employees of a customer who can then issue hard eIDs for the end-users. Furthermore, *XiTrust* offers also **workshops to train people** so that they can operate the service at least most of the time.

Pain Relievers for the End-Users
The two most important pain relievers for the end-users are that **secure channels are used for transmitting data** and that the **documents are stored encrypted** so that no other person is able to get their data. Another important pain reliever for the end-users is that the software **has gone through many tests** so that the possibility of a faulty service decreases. It would also be very important for them that the **data get stored in a trusted and certified data center** so they do not need to be afraid that their data get abused. A pain reliever that is also quite important is that it is **clearly defined in the SLA's which parties will be involved** so that the end-users know who will receive the data.

Gain Creators for the End-Users
The most important gain creator for the end-users is that they can **ease their daily business** with this software solution. The second most important gain creator is to **sign everywhere and any time** as this means that the end-users do not need to be in the office at a specific time for signing the documents. Another gain creator is that one person can **sign many documents at the same time** which is very convenient as the end-users only need to go through the signing process once and sign thereby many documents. Furthermore, **many people can sign one document within a short time** which saves a lot of time. Thus also this gain creator received a high rating. It is very convenient that the end-users always have an **overview over the document status**, meaning that they can see how many people have already signed the document at any time. The last two gain creators relate to the **usability** of *XiTrust MOXIS* and that **the service is structured in a way that it is self-explanatory,** which is very convenient and saves a lot of time.

6.3.3. FIT between the Value Map and the Customer Profile of the end-user

The FIT between the customer profile and the value map for the end-users is shown in figure 17. The FIT between the products & services and the customer jobs:

- *XiTrust MOXIS* fits perfectly to **sign documents** and **getting required signatures from others** as *XiTrust MOXIS* is an electronic signature file, with which it is possible to sign many documents in one minute and it facilitates the process of getting signatures form others as well. Furthermore, *XiTrust MOXIS* uses cryptographic concepts and handles sensitive data in a secure manner. For this reason, the customer job **protect personal information** is

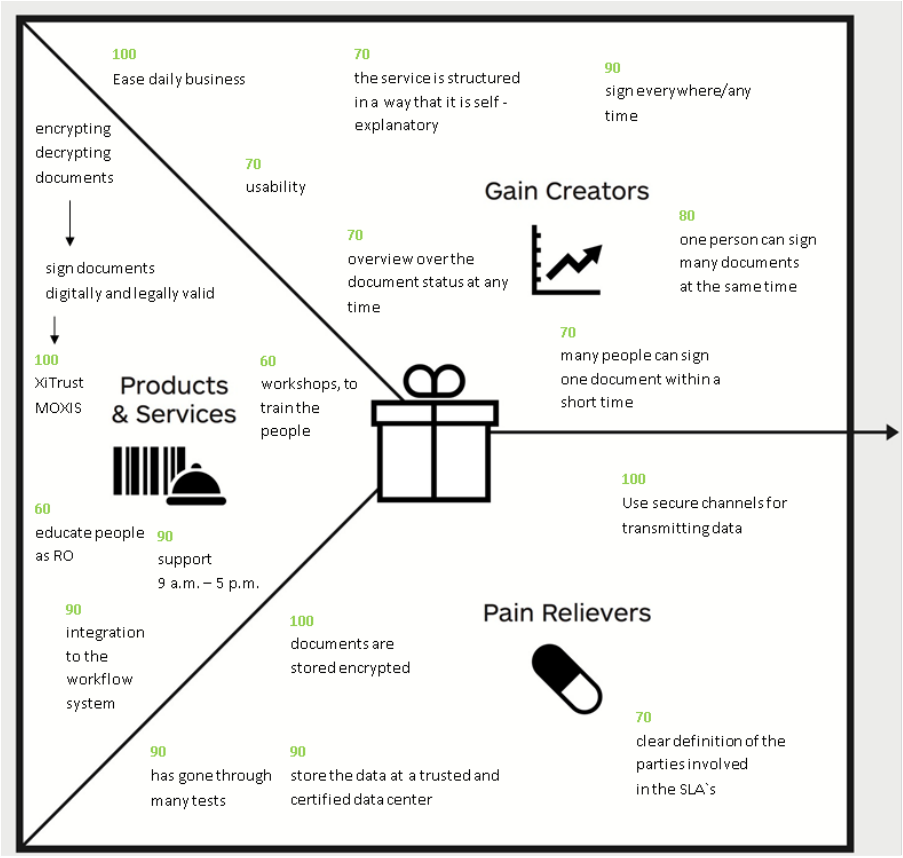
100
Ease daily business
70
the service is structured in a way that it is self - explanatory
90
sign everywhere/any time
encrypting decrypting documents
70
usability
Gain Creators
70
overview over the document status at any time
80
one person can sign many documents at the same time
sign documents digitally and legally valid
100
XiTrust MOXIS
Products & Services
60
workshops, to train the people
70
many people can sign one document within a short time
100
Use secure channels for transmitting data
60
educate people as RO
90
support 9 a.m. – 5 p.m.
90
integration to the workflow system
100
documents are stored encrypted
Pain Relievers
70
clear definition of the parties involved in the SLA`s
90
has gone through many tests
90
store the data at a trusted and certified data center

Figure 16.: The value map of *XiTrust* for the end-users (own illustration based on Osterwalder et al. (2014))

also covered.

The FIT between the pain relievers and the pains:

- Documents are stored encrypted and use secure channels for transmitting data: These relievers fit the pain that **personal data gets lost or abused**. The fear that **the service is not trustworthy** can also be taken away as the whole process, a document will go through, is secured by secure channels and the documents themselves are also encrypted.
- Went through many tests: Fits perfectly to **faulty services** and to **service does not work**. *XiTrust MOXIS* runs already in many big companies and before it will be sold as a cloud service, *XiTrust MOXIS* will be tested in-house and under runtime-conditions within a research project.
- Store the data at a trusted and certified data center: This pain reliever fits to the pain **not trustworthy** and solves the problem that the end-users **did not know who will receive their data**. *XiTrust* will clearly communicate, who the subcontractors are. *XiTrust* will also make sure that the data center, where *XiTrust MOXIS* will run, is ISO certified and the whole

data center is redundant.

- Clear definition of the parties involved in the SLAs: Fits also to **do not know who will receive my data**.

The FIT between the gain creators and the gains:

- Ease daily business: Fits perfectly to **getting signatures from others faster, sign any time, sign fast and straightforward, good usability, more convenient, sign everywhere, see if signatures are valid by verification tools** and **self-explanatory**. With *XiTrust MOXIS*, all required signatories get the document immediately after they have been invited and the process of signing takes only a minute. Furthermore, *XiTrust MOXIS* is a web application and can be accessed from any device, any time. These are the reasons why *XiTrust MOXIS* eases the daily business as it is possible to sign any time, everywhere fast and straightforward and, therefore, it is also possible to get the signatures from others faster.
- Sign everywhere/any time: This gain creator fits to the gains **sign any time** and **sign everywhere**. Many business people travel a lot and, therefore, it is very important for them to be location and time-independent. This fits perfectly to the gain creators of *XiTrust MOXIS*.
- The service is structured in a way that it is self-explanatory: Fits perfectly to **self-explanatory, good usability** and also a bit to **sign fast and straightforward**. The customers want a cloud service because they want to gain flexibility and they do not want to read a documentation before they can get started, which also fits to the gain creators of *XiTrust MOXIS*.
- Usability: Clearly fits to **good usability, self-explanatory, more convenient** and **sign fast and straightforward**. A self-explanatory service with a good usability is very important for customers. *XiTrust MOXIS* has gone through many iterations in which it was tested and redesigned and therefore, also this gain can be supported.
- Overview of the document status at any time: Is definitely a gain for the end-users and fits to **more convenient**. *XiTrust MOXIS* provides a status for each signature job, so everybody involved in this signature job knows always how many people have signed the document and who still has to sign the document.
- Many people can sign one document within a short time: Fits perfectly to **getting signatures from others faster**. This can easily be achieved with *XiTrust MOXIS* as after a document has been uploaded all the required signatories have it in their electronic signature file and it takes just one minute to sign.

The other four value maps and customer profiles are only slightly different than this one, so they are not described here but can be found in the appendix A. Those four value maps and customer profiles represent on the one hand the second role that is involved in the general business model, called *decision maker*, and on the other hand the roles *patient*, *hospital administration* and *doctor* for the eHealth domain business model. An arrow between two pains in the customer profile means that those pains relate to each other. After having finished all the value maps and customer profiles,

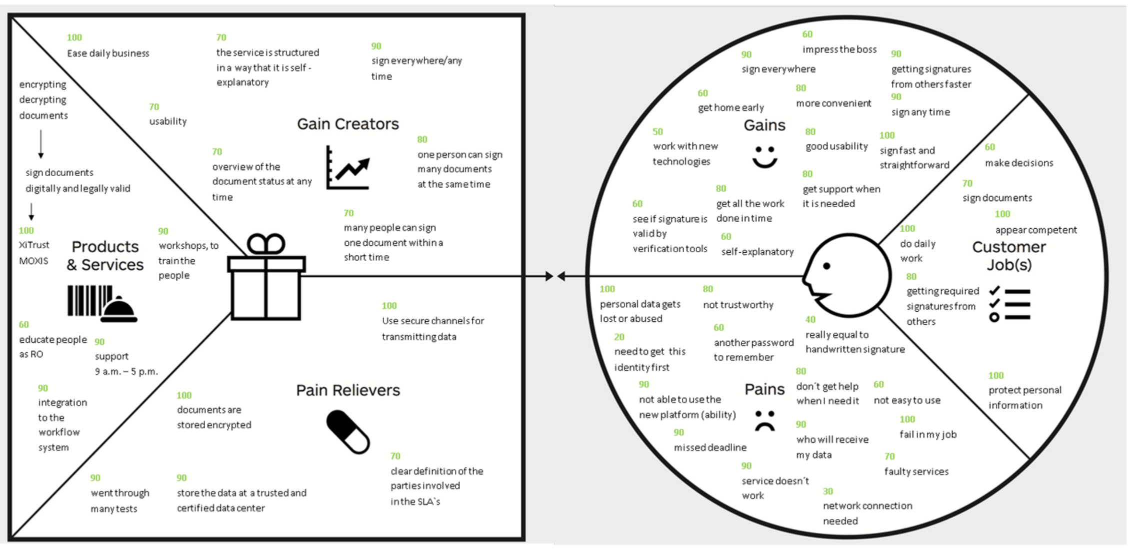
100
Ease daily business
70
the service is structured in a way that it is self - explanatory
90
sign everywhere/any time
encrypting decrypting documents
sign documents digitally and legally valid
70
usability
Gain Creators
80
one person can sign many documents at the same time
70
overview of the document status at any time
70
many people can sign one document within a short time
100
XiTrust MOXIS
Products & Services
90
workshops, to train the people
60
educate people as RO
90
support 9 a.m. – 5 p.m.
100
Use secure channels for transmitting data
90
integration to the workflow system
100
documents are stored encrypted
Pain Relievers
70
clear definition of the parties involved in the SLA`s
90
went through many tests
90
store the data at a trusted and certified data center
60
impress the boss
90
sign everywhere
90
getting signatures from others faster
60
get home early
80
more convenient
90
sign any time
Gains
50
work with new technologies
80
good usability
100
sign fast and straightforward
60
make decisions
80
get support when it is needed
80
get all the work done in time
70
sign documents
60
see if signature is valid by verification tools
60
self-explanatory
100
appear competent
100
do daily work
Customer Job(s)
80
getting required signatures from others
100
personal data gets lost or abused
80
not trustworthy
40
really equal to handwritten signature
60
another password to remember
20
need to get this identity first
100
protect personal information
80
don´t get help when I need it
60
not easy to use
Pains
90
not able to use the new platform (ability)
90
missed deadline
90
who will receive my data
100
fail in my job
70
faulty services
90
service doesn´t work
30
network connection needed

Figure 17.: FIT between the value map and the customer profile of end-users (own illustration based on Osterwalder et al. (2014))

they have been integrated to the different business models. The value maps of the end-user and the person who makes the decision if a product will be bought or not, have been integrated to the value proposition of the general business model. The customer profiles for the end-user and the decision maker have been integrated to the customer segments of the same business model. The value maps for the patient, the doctor and the hospital administration have been added to the value proposition of the eHealth domain business model. The customer profiles of the patient, the doctor and the hospital administration have been added to the customer segments of the eHealth domain business model.

6.4. Description of the Business Model Environment

The definition of the business model environment is inspired by the business model environment definition from *Osterwalder and Pigneur* as described in subchapter 2.4. The information in the following chapter was elicited during an interview with the CEO from *XiTrust Secure Technologies GmbH*. The environment was investigated from four different perspectives to gather all the important information.

Regarding the industry forces, the following information was gained:

- At the moment, no other company provides a digital bulk signature and signatures with such a quality that they are legally equal to a handwritten signature. Nevertheless, some digital signature solutions are emerging although the quality of these solutions are legally not on

such a high level. One example would be to sign a document with the iPad and a special pen and the signature is based on the hand movement. This solution might become a substitute because it is more convenient and might be legally sufficient for many people.
- Another important part of industry forces are all value chain actors which are in this case the registration officers and the company A-Trust.
- New competitors will appear with the eIDAS regulation.

Regarding the market forces, the following information was gained:

- In the short term, the market will be heading to the cloud. But as so often in the history, there are always ups and downs (things become popular but then they experience a downturn) and this might also happen with cloud computing. Another important fact to keep in mind is the country where cloud computing takes place. We, in Austria, live in a democratic state and people do not need to be afraid to go to prison or to get any other punishment for publishing their opinion or some personal information. This is different for people who are not living in a democratic state as they might be punished if they publish for example their opinion. For this reason, cloud computing will not work in those kind of countries and in the long term cloud computing is not seen as a solution that a lot of people will use for doing business.
- The most important customer segment is the one where a lot of customers already have a lot of their workflows digitized. Those customers are more likely to buy our product as they do not want to print their documents just to sign them and to scan them back in again. Furthermore, they are also already used to accomplish their tasks digital.
- Customers need solutions that lower their transaction costs and, therefore, *XiTrust* tries to lower these costs for their customers. The product *XiTrust Moxis*, for example, lowers the transaction costs in a way that people do not need to come to their office only for signing a document.
- The switching costs for customers of the *XiTrust GmbH* would be very low as they simply need to download and upload their documents at their new provider. At the moment, no other company provides the same products with the same quality.

Regarding the key trends, the following information was gained:

- Key technologies that enable big opportunities in the market of the company *XiTrust* are cloud computing and also the eIDAS regulation. But these trends will maybe become flops if people become suspicious and do not trust these technologies.

Regarding the macro economic forces, the following information was gained:

- At the moment, the economy in Austria is slightly growing but at the same time, the unemployment rate is growing as well.
- The funding situation in Europe is completely different than in the USA. In the USA it is common that you receive a lot of money when you simply present an idea. In Europe

you need to show that your idea works and that you already make profit before you receive funding. This fact makes it much harder for startups in Europe to enter new markets.

6.5. Service Lifecycle Map

The reason, why this service lifecycle map has been made was that *XiTrust* wanted to get an overview of the services that they already offer. Furthermore, they also wanted to know in which phases they could probably provide more services as they want to offer a complete package for the customer and not only a product. The information that has been gained from this service lifecycle map influenced also the business models. It was especially helpful for the channels block of the business model as they have been very clear after the development of the service lifecycle map. Additionally, the service lifecycle map was also quite helpful when the customer relationships and the key activities of the business model have been defined as they strongly relate with the service lifecycle map. The service lifecycle map is split up into four phases and displays the efforts that the company *XiTrust* performs in order to satisfy the needs of their customers, as shown in figure 18.

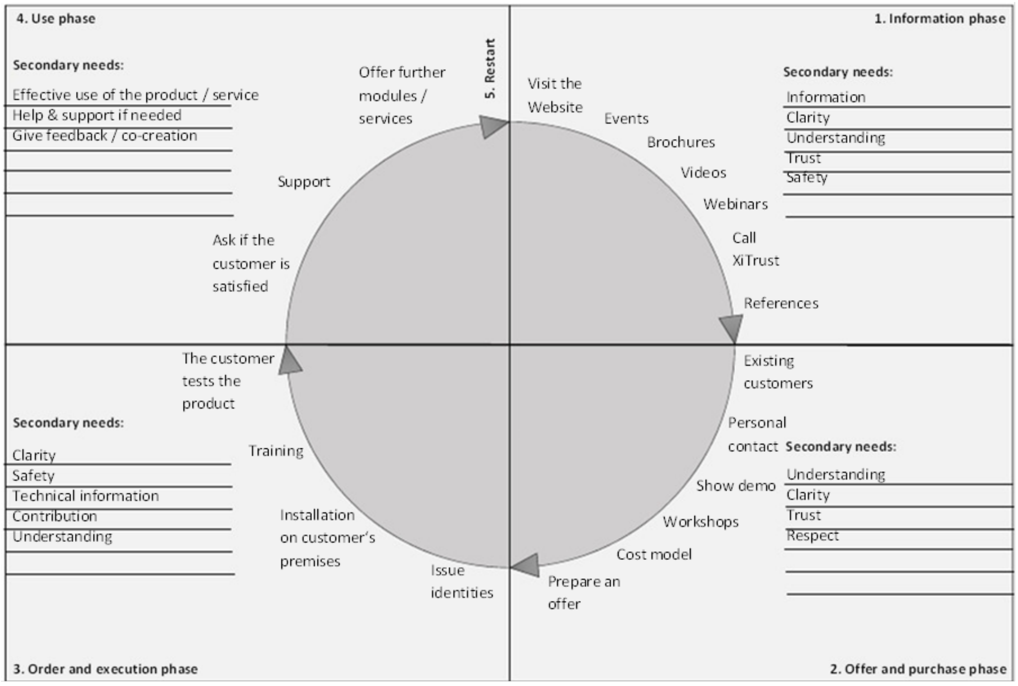

Figure 18.: Service lifecycle map of *XiTrust* (own illustration)

In the first phase, called *information phase*, the following secondary needs may arise:

- **Information** abut the products and services they offer.
- **Clarity** about how the products work.
- **Understanding** about how a specific product or service operates.
- **Trust** in the company including their products and services, and that personal data will not be abused.
- **Safety** that this company can solve the problems of the customer and, is therefore, the right choice.

The following efforts are performed by the company *XiTrust* to satisfy the secondary needs from above:
For getting a first impression of the products and services from *XiTrust*, a look at the **website** of *XiTrust* might be helpful or if some questions appear, a visit at one of the **events** where *XiTrust* is present might be a good idea. Furthermore, different **brochures** will be available during these events, which also provide a good overview over all the products and services of *XiTrust*. If visiting an event is not possible, *XiTrust* also provides some **videos** that can be viewed on the Internet or if a more interactive channel is requested, *XiTrust* offers **webinars** as well. In case none of the channels mentioned above is suitable, a customer can simply **call *XiTrust***. Last but not least, having a look at the **references** might be a good idea to see who is already a customer of *XiTrust*.

In the second phase, called *offer and purchase phase*, the following secondary needs may arise:

- **Understanding** about all the system components and the costs.
- **Clarity** about the corporate culture and how the products and services of *XiTrust* will solve the problems of the customer.
- **Trust** that *XiTrust* will give good advice and that their products really solve the problems of the customer.
- **Respect** towards customer requests.

The following efforts are performed to get a deeper understanding of the different products and services and to satisfy the secondary needs of this phase:
An opportunity that is not offered by *XiTrust*, but probably always a good choice, is to ask **existing customers** of *XiTrust*. In order to get a deeper understanding of the products and services it might be required to get in **personal contact** with an employee from *XiTrust*. During these personal meetings a *XiTrust* employee can **show a demo** of the product the customer is interested in. If a customer wishes that more employees of his/her company get a more detailed knowledge about a specific product, a **workshop** can be organized as well. If the customer is interested in buying the product, a *XiTrust* employee will show him/her the **cost model** and **prepare an offer** in the next step.

In the third phase, called *order and execution phase*, the following secondary needs may arise:

- **Clarity** about the usage of the service.
- **Safety** that the issuing and the usage of the identities works out.
- Better **understanding** of the chosen product and how it will solve the problems.

The following efforts are performed by the company *XiTrust* to satisfy the secondary needs of this phase:
All people who will use the software need to get a hard eID first and, therefore, *XiTrust* offers the service to **issue identities**, which only takes 10 minutes. After everything has been prepared, the product can be accessed by the customer and a **training** can be carried out. The customer is now in the situation that he/she can **test the product** and with this step the order and execution phase ends.

In the fourth and last phase, called *use phase*, the following secondary needs may arise:

- **Effective use of the product/service** that the product/service solves the problem and the customer can use it.
- **Help and support if needed** that the customer gets help when the software does not work as expected.
- **Give feedback/suggestions** so the customer can give feedback about the product/service and make suggestions if a feature is missing or does not work as expected.

The following efforts are performed by the company *XiTrust* to satisfy the secondary needs of this phase:
In order to ensure that the customer is satisfied with all the products/services from *XiTrust*, their employees call the customers regularly and **ask if they are satisfied**. Furthermore, *XiTrust* offers a **support** hotline which is staffed from 9 a.m. to 5 p.m. every work day. Last but not least, after the customer has been using the product for some time, an employee from *XiTrust* will call and ask if he/she needs **additional modules/services**.

6.6. General Business Model for XiTrust MOXIS in the Cloud

In the following paragraphs the general business model for *XiTrust MOXIS* in the cloud is described and shown in figure 19.

Key Partnerships

One of the key partners for *XiTrust MOXIS in the cloud* is the ***A-Trust GmbH***. *A-Trust* is an accredited TrustCenter that issues the qualified certificates and stores the private keys for people who use their mobile phone for signing documents with a qualified electronic signature.

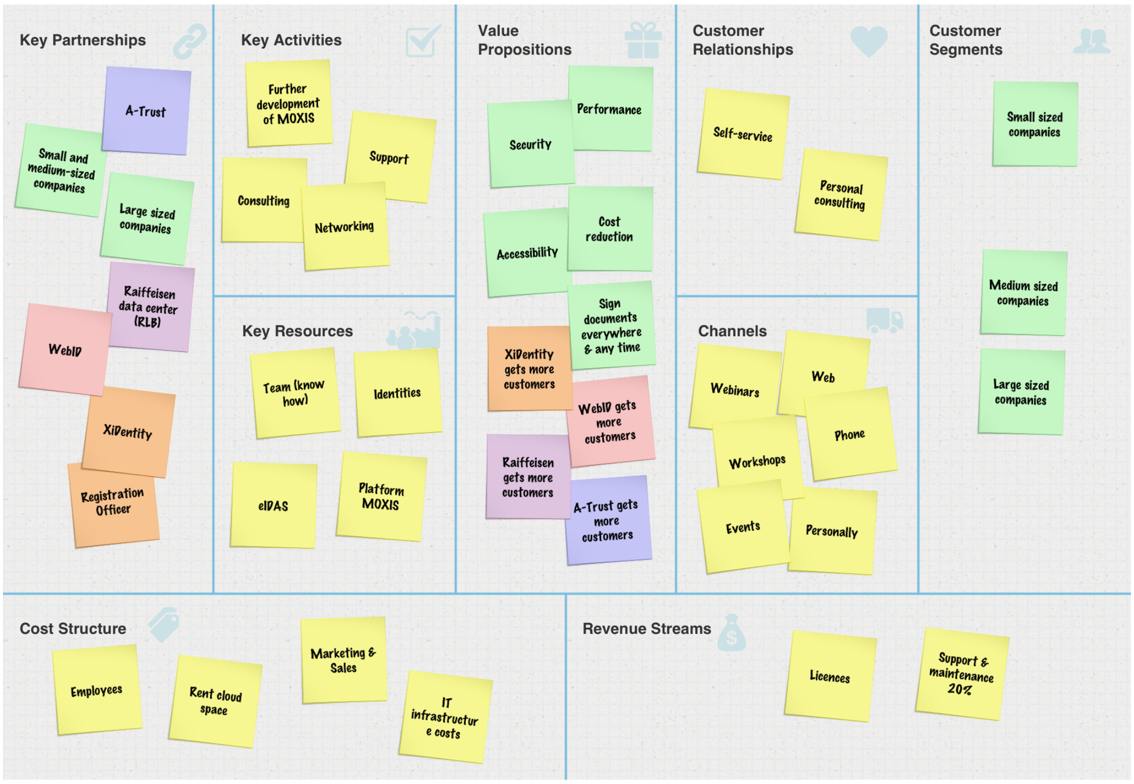

Figure 19.: General business model of *XiTrust MOXIS* in the cloud (own illustration based on Osterwalder and Pigneur (2010))

Another important key partner is ***Raiffeisen International Bank AG*** as they can provide a data center with a high level of security and availability. For this reason, the software solution *XiTrust MOXIS* will run in this data center and all the documents which customers require are also stored there.

The company ***XiDentity***, a subsidiary of *XiTrust GmbH*, is also an important partner as they can equip people from all over Europe with an electronic identity that is valid all over Europe. This identities can then immediately be used to sign documents legally valid.

Additionally to *XiDentity*, people can get their identities also from other people, but those people need to be certified ***registration officers***. This means that a person who wants an electronic identity needs to visit this *registration officer* physically, prove his/her identity and must have a mobile phone or citizen card. The electronic identity from a *registration officer* can also be used right after the registration process.

Another way to get an electronic identity is offered by the company ***WebID***. This option requires no physical meeting with the *registration officer*. The process of getting an identity with

WebID looks like this:
The person who wants to get an identity simply proves his/her identity by presenting his/her driving licence or passport in a Skype call. The person needs to show his/her identity card through the camera so that the person, who is responsible for the registration, can see the card.

Furthermore, our customer segments ***(small, medium and large sized companies)*** are also our key partners as they are hopefully satisfied with *XiTrust MOXIS* and thus they recommend the company *XiTrust*.

Key Activities

An important key activity is the **further development of the platform XiTrust MOXIS** as bugs need to be resolved continuously and new features need to be implemented to stay competitive.

Another important key activity is **support** because customers want to ask somebody when they have any problem with *XiTrust MOXIS*. For this reason offers *XiTrust* help for their customers every day from 9 a.m to 5 p.m.

Besides giving support it is also important to offer **consulting** especially before buying and installing the software in order to provide the customer with the perfect solution to his/her problems.

The activity **networking** is probably the most important one because getting in contact with new people regularly ensures that the customer base will grow faster. Furthermore, it is also important to maintain close contact to other industry partners and universities as these contacts might, for example, be the chance to work together in a new project.

Key Resources

The key resource that is the cornerstone of this signature service in the cloud is probably the **eIDAS regulation**. It defines that electronic identities, which have been issued in one European member state, are valid in all European member states. The regulation further defines that the certificate does not need to be under the sole control of the owner and, therefore, the certificate can be stored at a TrustCenter, which makes using the mobile phone signature possible. Furthermore, the regulation defines that companies are also able to authenticate their assets nowadays with a so called *electronic seal* and, therefore, no natural person, who functions as a representative of the company, is needed.

Another key resource are the **electronic identities** which are necessary to sign digitally and legally valid. A person can get this electronic identity, or also known as hard electronic identity, as defined in Zarsky and Andrade (2013), from the *Xidentity, WebID* or from a *registration officer*.

A key resource, which is necessary to develop a signature service, are people who have the knowledge to implement such a service and, therefore, **the team** of the company *XiTrust* is very important.

Last but not least, the **platform XiTrust MOXIS** itself, is one of the key resources. It enables customers to sign their documents everywhere, any time and, therefore, makes the process of signing much more convenient.

Value Propositions

The value proposition **sign documents everywhere and any time** is the most important value proposition for the two customer segments as it enables them to sign very convenient and without the need to be at a specific place at a specific time. In order to accomplish this, the digital signature service *XiTrust MOXIS* is needed as this service enables the user to digitally sign documents and these signatures are even legally valid. Another service that *XiTrust* offers is support during the business hours so that their customers get help whenever they need it. Furthermore, they also offer workshops for their customers so that they can get the maximum out of *XiTrust MOXIS*.

Another value proposition that *XiTrust* offers is **performance**, because many people can sign a document within a short time and documents do not need to be printed and scanned again. These characteristics can be reached because of the gain creators, such as **one person can sign many documents at the same time**, **many people can sign one document within a short time** and **sign everywhere/any time**.

The fact that people do not need to print documents and scan them again speeds up the whole process and, therefore, **cost reduction** is another value proposition. This cost reduction can be achieved with the service *XiTrust MOXIS*, which enables the customer to digitally sign documents.

Furthermore, a higher **accessibility** can be provided as the signature service is a web service and so signing from every device, at any time and everywhere is possible. This also corresponds with the value map or more precisely with the gain creator **sign everywhere/any time**.

The value proposition **security** can be offered with the help of many cryptographic mechanisms in place but not only *XiTrust* guarantees security. Also their subcontractors, such as *Raiffeisen International Bank AG*, have a lot of mechanisms in place to protect all the user data. This value proposition can be provided with the service *XiTrust MOXIS* as it encrypts all the documents and the pain relievers **use secure channels for transmitting data**, **documents are stored encrypted**, **has gone through many tests** and **store the data at a trusted and certified data center** as stated in the value map.

In order to also provide a value proposition for the key partners ***A-Trust, XiDentity, Raiffeisen*** and ***WebID***, *XiTrust* assures to advertise them so that they might **get more customers**. [2]

[2] *Registration officers* are not included here as it is assumed that they work for one of the customer segments.

Customer Relationships

The main customer relationship is **self-service** as the customer can upload the documents by himself/herself and also sign the documents on his/her own.

The second customer relationship that is offered by *XiTrust* is **personal consulting**. This service can be perceived for money.

Channels

In order to get a first impression of the company *XiTrust* and their services, the potential customer should browse the **web** and have a look at the company's web page. The channel **webinars** is especially interesting for potential customers. With this channel, customers can get great insights into the different services from *XiTrust* within an hour.

Another good channel for potential customers are different **events**. *XiTrust* is present at different fairs and also organizes different kinds of events where employees from *XiTrust* are available and explain the services that they provide.

A channel which is interesting for potential customers as well as for existing customers is the **phone** because potential customers can get more detailed insights of the products that *XiTrust* offer, and existing customers can ask for help if they have a problem with a product from *XiTrust*.

After the customers have bought a product, *XiTrust* offers **workshops** in order to get started with the new software more easily.

Last but not least, if a customer has bigger problems and wishes to talk in more detail with a *XiTrust* employee, he/she can make use of the **personal** channel and can have an individual talk.

Customer Segments

Among the customer segments for the signature service in the cloud are **small and medium sized companies** as it is easier for them to pay a monthly rate instead of buying all the necessary infrastructure at the beginning.

Large sized companies are among the customers as they are good multipliers and can also be flagships, so getting new customers becomes easier.

Cost Structure

The costs for the signature service in the cloud consist mainly of the costs for the **employees** of *XiTrust* as those are recurring costs and the team of *XiTrust* consists of 23 persons at the moment and is growing rapidly.

Another big amount of money is channeled into **marketing and sales** as *XiTrust* is present at many fairs and also the other advertising measures are very costly.

Another part, which is not as costly but still needs to be considered, is the **IT-infrastructure and its costs** because all the employees need hardware that is appropriate for developing a software that should run in the cloud.

Furthermore, the **rent** for the data center, where the software shell run, causes costs as well.

Revenue Streams

All the costs mentioned above need to be covered by the money earned from product sales. The earnings are thereby split up into **licenses** and **maintenance and support**. The license costs refer to the costs of *XiTrust MOXIS* and how many signature files are sold. The maintenance and support costs refer to the license costs and account for 20% of them.

6.7. EHealth Domain Business Model for XiTrust MOXIS in the Cloud

All building blocks of the eHealth domain business model for *XiTrust MOXIS* in the cloud are described in the following paragraphs. A representation of this business model is shown in figure 20.

Key Partnerships

The key partners for the hospital case regarding *XiTrust MOXIS in the cloud* are a bit different than for the general business model before. The reason for that is that data in a hospital context is very sensitive and, therefore, additional measures are requested by the hospitals. The **data center**, where the signature service should run and the documents are stored, should be located in the same city or at least in the same country as the hospital.

The other key partners such as **A-Trust, XiDentity, registration officers** and **WebID**, which have already been described for the general business model, stay the same.

Key Activities

The four key activities from the general business model are basically the same in the eHealth

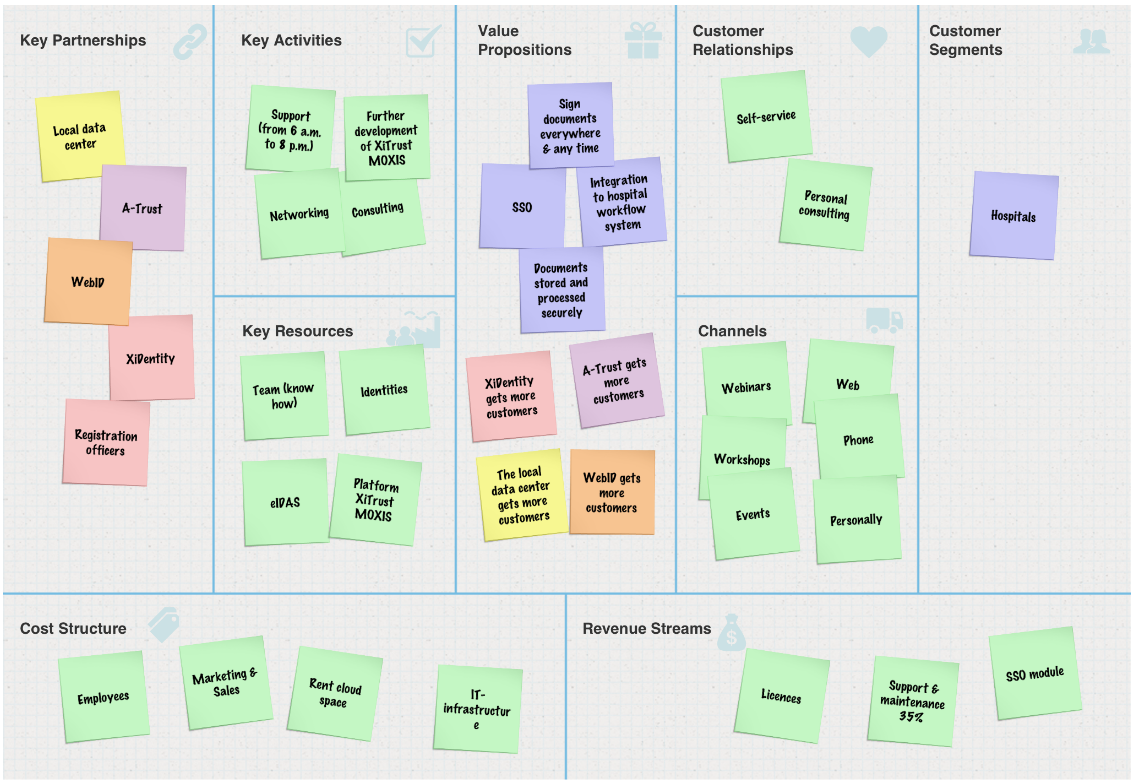

Figure 20.: Business model for the eHealth domain (own illustration based on Osterwalder and Pigneur (2010))

domain business model. The only difference is that the **support** hours changed as hospitals operate every hour, every day. For this reason, the support hours are from 6 a.m. to 8 p.m. instead of 9 a.m. to 5 p.m., so that the nurses and doctors in each shift have the opportunity to call.

The other key activities such as **further development of *XiTrust MOXIS*, consulting** and **networking**, stay the same.

Key Resources

All the key resources **(team, identities, eIDAS and platform XiTrust MOXIS)** of the general business model are equal to the key resources of the eHealth domain business model.

Value Propositions

Besides the value propositions that **XiDentity, A-Trust, WebID and the local data center get more customers** and that customers can **sign documents everywhere and any time** the following three value propositions have been added for the eHealth domain business model:

- Sometimes doctors do not have much time and they already have to remember a lot, so they do not want another password that they have to remember. Therefore, *XiTrust* offers an additional module called **SSO** for their digital signature service *XiTrust MOXIS*.

- Furthermore, *XiTrust* offers a total **integration to the hospital workflow system** so that the users do not need to switch between the different systems.
- As documents are very sensitive in a hospital context, *XiTrust MOXIS* offers that all the **documents are stored and processed securely**.

Customer Relationships

The two customer relationships **(self-service and personal consulting)** of the general business model are equal to the customer relationships of the eHealth domain business model.

Channels

All the channels **(webinars, web, workshops, phone, events and personally)** of the general business model are equal to the channels of the eHealth domain business model.

Customer Segments

The customer segments of the eHealth domain business model are completely different to those of the general business model because instead of three customers segments, it consists only of one customer segment: **hospitals**.

Cost Structure

The cost structure with the following four cost items **employees, marketing and sales, rent for cloud space and IT-infrastructure** of the general business model are equal to the cost structure of the eHealth domain business model.

Revenue Streams

Besides the revenue streams **(licenses, maintenance** and **support)** of the general business model, an additional revenue stream for the eHealth domain business model needs to be added, as the **SSO module** causes separate costs.

7. Recommendations for Action

In this chapter, measures that need to be taken in order to provide *XiTrust MOXIS* in the cloud are described and also the milestones that need to be reached to successfully provide a signature service in the cloud. Additionally, these milestones are presented in an chronological order.

7.1. Measures to be taken

The measures that need to be taken have been elicited from the expert interviews, literature research and different employees from *XiTrust*, who are strongly involved in the software development process. The following section is structured in a way that first of all, general measures are described. Afterwards, the topics identities, multi client capability in general, and how multi client capability effects the database as well as the different signature qualities (signing/releasing), are described. Furthermore, a handling for unauthorized users, multilingualism and support is suggested.

7.1.1. General Measures to be taken

A really important goal is to be very transparent, starting from the first touch point a customer has with the company *XiTrust*. The reason for that is that the company *XiTrust* first of all needs to win the customer's confidence in order to sell a product or service. This is especially in this case important as the company *XiTrust* wants to sell products and services that use privacy sensitive data and operate in the cloud. The actions that can be taken to gain the trust of customers are:

- Customers have to be informed about the companies that receive their data.
- Customers also have to get informed about where and how their data is stored.
- According to a survey in Horvath and Agrawal (2015), customers have to learn about the products of the cloud service provider, data safety and also have to be trained in that area.
- Furthermore, a contract with all parties involved is necessary to define for which purpose the data will be used. This contract also needs to include which rights and obligations every party has.

In order to show the customer that everything is very transparent and nobody wants to conceal information from him/her, the online terms and conditions should be short and easy to understand. These are things that can already be done before the customer signs an offer but there should also exist possibilities for the customer to check if he/she really gets what was promised in the SLA and in the online terms and conditions. For this reason, the customer should be able to check how much he/she has used the service and should have the right to audit *XiTrust* and their subcontractors.

7.1.2. Hard Electronic Identity

Nevertheless, before a customer can even start using the digital signature service *XiTrust MOXIS* the customer needs to get a hard eID. The new eIDAS regulation, which fully came into force in July 2016, enables that these hard eIDs can be stored in a trusted data center and that hard eIDs that have been issued in a European member state are valid in all other European member states. The fact that hard eIDs can be stored in a trusted data center enables the people to use the mobile phone signature. This simplifies the problem of identity provisioning all over Europe for the company *XiTrust* extremely. Now, their subsidiary *XiDentity* and their partners *A-Trust* and *WebID* only need to equip people with hard eIDs and then people can start using the service all over Europe.

7.1.3. Multi-Client Capability

The most important property that *XiTrust* needs to obtain is mulit-client capability. This starts already when the customer wants to reach the service because every customer should get his/her own URL. For the company called *XY* the URL could be like this: *https://xy.xitrust.com/moxis/*.

The next step, where multi-client capability is important, is when the customer sees all the possible placeholders he/she can choose from. These placeholders are stored in a database and are different for every customer. To get *XiTrust MOXIS* ready for the cloud, the placeholders need to be linked to a specific customer. This means that every company has a set of specific placeholders and every user who signs with *XiTrust MOXIS* within this company gets his/her own placeholder and sees only the company specific placeholders. Furthermore, the administrator of the respective company should be able to create, change and delete placeholders. Additionally, the administrator should be able to define an e-mail address when creating such a placeholder. This person should then get an invite via e-mail and only this person should be able to sign in the place of this placeholder.

7.1.4. Database

The fact that one database needs to handle many different customers requires that also the database needs to become multi-client capable. According to Chong (2012), six different approaches exist to design a database for multi-client capable. The most interesting approach probably is, where one database is used but with different schemas. This means that you still need only one database but the data is better isolated because a different set of tables with a different schema name is used. An advantage of this solution is that the SQL statements need not to be changed principally; only the schema name needs to be changed. A disadvantage is that more storage is needed this way because one set of tables per customer will be created.

7.1.5. Signing/Releasing Documents

Another feature that requires multi-client capability is that the customer has the choice to sign or simply release a document. This means that the information, if a user can sign and release or only sign or only release documents, needs to be user specific. This problem could be solved by storing that information in the database or with providing two different versions of *XiTrust MOXIS*. *XiTrust* already rents resources at the *Raiffeisen data center*, in particular 100GB storage, 2 GHz CPU and 6 GB RAM. As this space is already partially used, maximal two instances of *XiTrust MOXIS* can be installed additionally. For this reason, a standard and a premium version could be installed. The standard version could then cover a plain *XiTrust MOXIS* with which it is only possible to sign documents and a premium version which covers a *XiTrust MOXIS* with all modules including the module for releasing documents.

7.1.6. Unauthorized Users

If a person, who does not have a signature file, needs to sign a document he/she needs to be invited and receive a general placeholder from the inviting person. After the customer has typed in more than three letters, *XiTrust MOXIS* suggests e-mail addresses and these e-mail addresses need to be customer specific. In order to provide this feature also when offering the service in the cloud, a linkage between these e-mail addresses and the customer need to be created. Afterwards, the user can finish this task and the people who need to sign the document get an invite by e-mail with a link to the platform *XiTrust MOXIS*. One solution to realize these two linkages is to store all placeholders and e-mail addresses that are available for this specific customer in the database schema.

7.1.7. Multilingualism and Support

Furthermore, a logic regarding the usage of different languages needs to be considered. Especially when people who are from different countries sign a document together. If one client invites people who have different mother tongues, the e-mails with the invite to sign can either be in English or it needs to be indicated, which user prefers, which language for the e-mail. Additionally, the user also needs the possibility to switch the language within the application easily.

Last but not least, additional employees will be needed to cover the extended support times.

7.2. Specifying Milestones

In the following section, all important milestones are listed and presented in figure 21. These milestones are divided into the same subcategories as the measures that have to be taken.

Database

- A decision is needed how to make the database multi-client capable.

Signing/Releasing Documents

- The next step is to decide if two different versions of *XiTrust MOXIS* should be provided. One version would then consist of a standard *XiTrust MOXIS* and one would consist of a premium *XiTrust MOXIS*, whereby it needs to be defined which modules are included in which version.
- Thereafter, a decision regarding the signature quality needs to be made for each *XiTrust MOXIS* version. Shall users of the standard version only be able to sign and users of the premium version will be able to sign and release documents?

Multi-Client Capability

- Now, a logic for the placeholders and the QR Codes is needed in order to make them multi-client capable.
- In a next step, it needs to be defined how unauthorized users will be invited to sign a document if the service runs in the cloud and needs to be multi-client capable.
- Every customer needs to get his/her own URL. An example for the company *XY* would be *https://xy.xitrust.com/moxis/*.

Multilingualism and Support

- If an unregistered user wants to sign a document, a logic for different languages is necessary. The language of the invitation e-mail for unregistered users needs to be defined. Registered users should have the possibility to change the language.
- Another important step is to hire additional staff for the support team in order to handle the extended support times.

General Milestones

- Furthermore, a tool with which the customers can check how actively they have used the different services needs to be implemented.
- Last but not least, the online terms and conditions need to be defined in a short and understandable way.

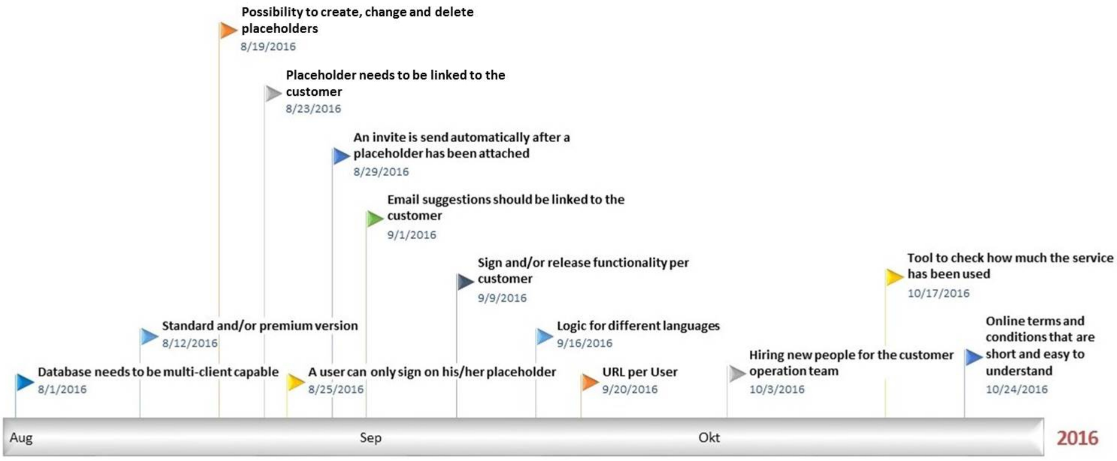

Figure 21.: Milestones for preparing *XiTrust MOXIS* for the cloud (own illustration)

8. Summary and Future Work

Business models are the cornerstone for achieving and creating new business areas. By designing the business models carefully and getting aware of the possibilities that business models offer, companies can detect failures in their plans for new products and services much earlier and this makes business model innovations much more successful. For this reason, the company *XiTrust* decided to create a business model for their idea to provide *XiTrust MOXIS* in the cloud.

Within this master thesis, two business models have been developed. One focusing on the provision of *XiTrust MOXIS* in the cloud for companies of different sizes, and one focusing on the provision of *XiTrust MOXIS* in the cloud for the eHealth sector. In order to get started with the development of these two business models, different customer profiles and value maps of different customer groups have been prepared. To accomplish a complete picture of the services that *XiTrust* offers for their customers, a service lifecycle map has been created as well. Furthermore, organizational, technical and legal requirements have been defined, which need to be fulfilled to provide *XiTrust MOXIS* in the cloud in a way that the customers can easily and securely carry out their tasks.

Now, the requirements need to be discussed in detail with the developers of the company *XiTrust* and a holistic concept needs to be created. In a next step, stories need to be defined so that the product owner is able to set up a plan for their scrum process. After all the stories are implemented, a first prototype can be installed in a testing environment. This prototype needs to be tested so that it is clear that it fulfills the requirements of an application in the cloud. This whole development process will need further iterations before the service is ready for the market.

XiTrust has already received feedback from some of their customers, that they would be interested in *XiTrust MOXIS* in the cloud but while the development team is implementing the service, the marketing department needs to spread the information about the new service. The sales department needs to present and explain the new service when they meet the customers and the human resources department needs to search for new employees so that *XiTrust MOXIS* in the cloud will become a successful service for *XiTrust* soon.

References

Alaqra, A., Fischer-Hübner, S., Pettersson, J. S., van Geelkerken, F., Waestlund, E., Vokamer, M., Länger, T., and Pöhls, H., 2015. Legal, Social and HCI Requirements. *Deliverable within the PrismaCloud project for Privacy and Security Maintaining Services in the Cloud.* URL `www.prismacloud.eu`.

Amit, R. and Zott, C., 2001. Value Creation in E-Business. *In: Strategic Management Journal*, pages 493–520.

Aschbacher, H., 2014. Framework für das agile Entwickeln von IKT basierten Dienstleistungen unter Nutzung von Smart Services. Master's thesis, Technische Universität Graz.

Atos Spain, 2008. STORK 2.0 - Secure Identity Across Borders Linked. URL `https://www.eid-stork2.eu/`. visited: 24.8.2015.

Ayoub, R., 2013. Protecting the Cloud - Fortinet Technologies and Services that Address Your Cloud Security Challenges. URL `https://downloads.cloudsecurityalliance.org/vendor_papers/Protecting-the-Cloud-Robert-Ayoub.pdf`.

Badger, L., Grance, T., Patt Corner, R., and Voas, J., 2011. Cloud Computing Synopsis and Recommendations. *Recommendations of the National Institute of Standards and Technology*. URL `http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf`.

Bitglass, 2014a. The Definitive Guide to Cloud Access Security Brokers. URL `http://www.ciosummits.com/Online_Asset_Bitglass_White_Paper_-_The_Definitive_Guide_to_Cloud_Access_Security_Brokers.pdf`. White paper.

Bitglass, 2014b. The 2014 Bitglass Healthcare Breach Report. URL `http://www.bitglass.com/resources#whitepapers=1&analyst_reports=1`.

Bundesamt für Sicherheit in der Informationstechnik, 2012. Sicherheitsempfehlungen für Cloud Computing Anbieter. URL `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile&v=6`. Eckpunktepapier.

Bundeskanzleramt, 2015. Gesamte Rechtsvorschrift für Stammzahlenregisterbehördenverordnung 2009, Fassung vom 30.09.2015. URL https://www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/20006487/StZRegBehV%202009%2c%20Fassung%20vom%2015.11.2016.pdf.

Chong, R. F., 2012. Designing a Database for Multi-Tenancy on the Cloud. URL http://www.ibm.com/developerworks/data/library/techarticle/dm-1201dbdesigncloud/. visited: 20.01.2016.

Columbus, L., 2014. Computerworld's 2015 Forecast Predicts Security, Cloud Computing And Analytics Will Lead IT Spending. URL http://www.forbes.com/sites/louiscolumbus/2014/11/26/computerworlds-2015-forecast-predicts-security-cloud-\computing-and-analytics-will-lead-it-spending/#6a49bdc6d777. visited: 17.8.2015.

Commvault, 2015. Your Top 5 Cloud Data Protection Challenges. Solved. URL https://kapost-files-prod.s3.amazonaws.com/published/555b8cbd52e434322e0001b7/top-5-cloud-data-protection-challenges-solved.pdf?kui=6abTGqXZvP-wdXicnT-gvA.

Digitales, O., 2015a. Das kann die Handy-Signatur. URL https://www.buergerkarte.at/anwendungen-handy.html. visited: 15.09.2015.

Digitales, O., 2015b. IKT-News. URL https://www.digitales.oesterreich.gv.at/documents/22124/38252/IKT-Newsletter-Juli-2015_signiert.pdf/28e93a1a-06e7-4fe6-bdf7-fa0f2b4ce4b7.

Digitales, O., 2014. Handy-Signatur & Bürgerkarte. URL http://buergerkarte.at/. visited: 1.9.2015.

Digitales, O., 2015c. Rechtliche Rahmenbedingungen von E-Government in Österreich. URL http://www.digitales.oesterreich.gv.at/site/5238/default.aspx#a11. visited: 26.08.2015.

Eriksdotter, H., 2010. SaaS versus Lizenzsoftware. URL http://www.computerwoche.de/a/unsicheres-einsparpotenzial,1933160. visited: 25.11.2015.

Foran, J., 2010. Cloud computing licensing: Buyer beware. URL http://searchcloudcomputing.techtarget.com/feature/Cloud-computing-licensing-Buyer-beware. visited: 17.8.2015.

Gassmann, O. and Csik, M., 2013. *Geschäftsmodelle entwickeln*. Carl Hanser Verlag, München.

Google, 2015a. The App Engine Standard Environment. URL https://cloud.google.com/appengine/docs/about-the-standard-environment. visited: 3.12.2015.

Google, 2015b. What is Google Cloud Storage? URL https://cloud.google.com/storage/docs/overview. visited: 3.12.2015.

Google, 2015c. Google Cloud Platform. URL https://cloud.google.com/. visited: 3.12.2015.

Harms, D., Heinen, E., Kuiper, K., Müritz, R., Nenninger, B., Otto, U., and Strina, G., 2009. *Dienstleistungen systematisch entwickeln. Ein Methoden-Leitfaden für den Mittelstand*. Itb-Institut für Technik der Betriebsführung im deutschen Handwerksinstitut e.V, Karlsruhe.

Heritier, C., 2014. OPENTRUST. URL https://www.opentrust.com/?lang=en. visisted: 25.8.2015.

Hodgson, G. M., 2003. Capitalism, Complexity, and Inequality. *In: Journal of Economic Issues*, pages 471–478.

Hoppe, K. and Kollmer, H., 2001. Strategie und Geschäftsmodell. *In: Meinhardt Y. (Hrsg.) Veränderung von Geschäftsmodellen in dynamischen Industrien: Fallstudien aus der Biotech-, Pharmaindustrie und bei Business-to consumer-Portalen. DUV*. Wiesbaden.

Horvath, A. and Agrawal, R., 2015. Trust in Cloud Computing. *In: Proceedings of IEEE SoutheastCon 2015*.

Hühnlein, D., Hornung, G., Roß nagel, H., Schmölz, J., Wich, T., and Zibuschka, J., 2011. SkIDentity - Vertrauenswürdige Identitäten für die Cloud. *In: DA-CH Security*, pages 296–304.

IBM, 2013. IBM cloud computing. URL http://cloud-computing-in-the-cloud.com/ibm-cloud-computing-wikipedia-article/59. visited: 2.12.2015.

IBM, G. K. T. L., 2015. IBM Cloud & Smarter Infrastructure Training. URL http://www.globalknowledge.net/mea-shared-content/documents/684697/886403/EMEA_IBM_CSI_Q1_2015_Web_KSA. visited: 2.12.2015.

IDCResearch, 2015. Worldwide Cloud IT Infrastructure Market Grows by 25.1Quarter on Growing Demand for Public and Private Cloud IT Services, According to IDC. URL http://www.idc.com/getdoc.jsp?containerId=prUS25732215. visited: 24.8.2015.

Jansen, W., Grance, T., et al., 2011. Guidelines on Security and Privacy in Public Cloud Computing. *In: NIST special publication*, 800(144).

Joneja, N., 2014. Bringing together the best of PaaS and IaaS. URL https://cloudplatform.googleblog.com/2014/03/bringing-together-best-of-paas-and-iaas.html. visited: 3.12.2015.

Knyphausen-Aufseß, D. and Zollenkop, M., 2011. Transformation von Geschäftsmodellen–Treiber, Entwicklungsmuster, Innovationsmanagement. *In: Bieger, T./Bickhoff, N./Caspers, R./Knyphausen-Aufseß, D./Reding, K. (Hrsg.) Innovative Geschäftsmodelle*, pages 111–128.

Krach, K., 2003. DocuSign. URL https://www.docusign.com/. visited: 26.8.2015.

Lambo, T., 2012. Why You Need a Cloud Rating Score. URL https://cloudsecurityalliance.org/wp-content/uploads/2012/02/Taiye_Lambo_CloudScore.pdf.

Leong, L., Toombs, D., and Gill, B., 2015. Magic Quadrant for Cloud Infrastructure as a Service, Worldwide. URL https://virtualizationandstorage.files.wordpress.com/2015/06/magic-quadrant-for-cloud-infrastructure-as-a-service-worldwide.pdf.

Liang, S. and Ulander, P., 2010. 7 Requirements for Building Your Cloud Infrastructure. URL http://www.cio.com/article/2412506/cloud-computing/7-requirements-for-building-your-cloud-infrastructure.html. visited: 8.10.2015.

Linden, F., 2008. Smart Open Services for European Patients. URL http://www.epsos.eu/. visited: 24.8.2015.

Maguire, J., 2015. Cloud Computing Market Leaders, 2015. URL http://www.webopedia.com/Blog/cloud-computing-market-leaders-2015.html. visited 3.12.2015.

Markey, S., 2011. Scanning Your Cloud Environment. URL https://cloudsecurityalliance.org/wp-content/uploads/2011/11/CSA_Scanning_Cloud_Environment.pdf.

Marko, W. A., 2014. Small-scale, Big Impact - Utilities' New Business Models for "'Energiewende"'. *In: Die Unternehmung - Swiss Journal of Business Research and Practice*, pages 201–220.

Martins, H., 2014. Expanding Health Data Interoperability Services. URL http://www.expandproject.eu/. visited: 25.8.2015.

McDonald, P., 2008. Introducing Google App Engine + our new blog. URL http://googleappengine.blogspot.co.at/2008/04/introducing-google-app-engine-our-new.html. visited: 3.12.2015.

Mcnee, B., 2014. Digital Business Rethinking Fundamentals. URL http://cbs2014.saugatucktechnology.com/images/Documents/Presentations/CBS14%20McNee%20Keynote%20-%20Cloud%20and%20Digital%20Business-12Nov2014.pdf.

Metz, C., 2012. The Cult of Amazon: How a Bookseller Invented the Future of Computing. URL `http://www.wired.com/2012/11/amazon-3/`. visited: 3.09.2015.

Morgan, T. P., 2014. A Rare Peek Into The Massive Scale of AWS. URL `http://www.enterprisetech.com/2014/11/14/rare-peek-massive-scale-aws/`. visited: 03.09.2015.

Morris, M., Schindehutte, M., and Allen, J., 2005. The Entrepreneur's Business Model: Toward a unified Perspective. *In: Journal of Business Research*, pages 726–735.

OASIS Provisioning Services Technical Committee, 2001. An Introduction to the Provisioning Services Technical Committee. URL `http://xml.coverpages.org/PSTC-Intro-102301.pdf`.

Osterwalder, A., 2004. The Business Model Ontology: A Proposition in a Design Science Approach. PhD dissertation, University of Lausanne, Switzerland.

Osterwalder, A. and Pigneur, Y., 2010. *Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers*. John Wiley & Sons, Hoboken, NJ.

Osterwalder, A., Pigneur, Y., Bernarda, G., and Smith, A., 2014. *Value Proposition Design: How to create Products and Services Customers want*. John Wiley & Sons, Hoboken, NJ.

Qian, L., Luo, Z., Du, Y., and Guo, L., 2009. Cloud Computing: An Overview. *In: IEEE International Conference on Cloud Computing*, pages 626–631.

Reed, A., Rezek, C., and Paul, S., 2011. Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. *Cloud Security Alliance*, 3. URL `https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf`.

Reese, G., 2009. *Cloud Application Architectures*. O'Reilly Media, Inc., Sebastopol, CA.

Roessler, T., 2012. PrimeSign. URL `https://www.prime-sign.com/`. visited: 20.8.2015.

Rouse, M., 2010. User Account Provisioning Definition. URL `http://searchsecurity.techtarget.com/definition/user-account-provisioning`. visited: 20.09.2015.

Rundfunk und Telekom Regulierungs-GmbH, 2015. Recht. URL `https://www.signatur.rtr.at/de/elsi/Recht.html`. visited: 24.08.2015.

Schallmo, D. R., 2013. *Geschäftsmodelle erfolgreich entwickeln und implementieren: Mit Aufgaben und Kontrollfragen*. Springer-Verlag, Berlin.

Shields, A., 2014. Why Microsoft appears to be on the path to future success. URL http://marketrealist.com/2014/08/microsoft-appears-path-future-success/. visited: 28.09.2015.

Slamanig, D., Stranacher, K., and Zwattendorfer, B., 2014. User-Centric Identity as a Service-Architecture for eIDs with Selective Attribute Disclosure. *In: ACM Symposium on Access Control Models and Technologies (SACMAT)*, pages 153–164.

Srinivasan, M. K., Sarukesi, K., Rodrigues, P., Manoj, M. S., and Revathy, P., 2012. State-of-the-art Cloud Computing Security Taxonomies - A classification of security challenges in the present cloud computing environment. *In: Proceedings of the International Conference on Advances in Computing, Communications and Informatics - ICACCI '12*, pages 470–476.

Sullivan, D., 2005. *The definitive guide to security management.* Realtimepublishers, Santa Rosa, CA.

Sultan, N. A., 2011. Reaching for the "cloud": How SMEs can manage. *In: International Journal of Information Management*, pages 272–278.

Suzic, B., 2015. E-ID in the Cloud with SCIM. URL https://demo.a-sit.at/wp-content/uploads/2015/03/Studie_eID_SCIM_Cloud_1.0.pdf.

Teece, D. J., 2010. Business Models, Business Strategy and Innovation. *Long range planning*, pages 172–194.

The European Parliament and the Council of the European Union, 2014. Regulation (EU) No 910/2014 of the European Parliament and of the Council. URL http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN.

Weiner, N., Renner, T., and Kett, H., 2010. *Geschäftsmodelle im" Internet der Dienste".* Fraunhofer-Verlag, Stuttgart.

Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., Meinl, T., Michalk, W., and Stößer, J., 2009. Cloud-Computing–Eine Abgrenzung, Geschäftsmodelle und Forschungsgebiete. *In: Wirtschaftsinformatik*, 51(5). Springer Gabler, Wiesbaden.

Wirtz, B. W., 2010. Business model management. *Gabler Verlag, Wiesbaden.*

Zarsky, T. Z. and Andrade, N. N. G. D., 2013. Regulating Electronic Identity Intermediaries: The "Soft eID" Conundrum. *In: Ohio State Law Journal*, pages 1335–1400.

A. Customer Profiles and Value Maps

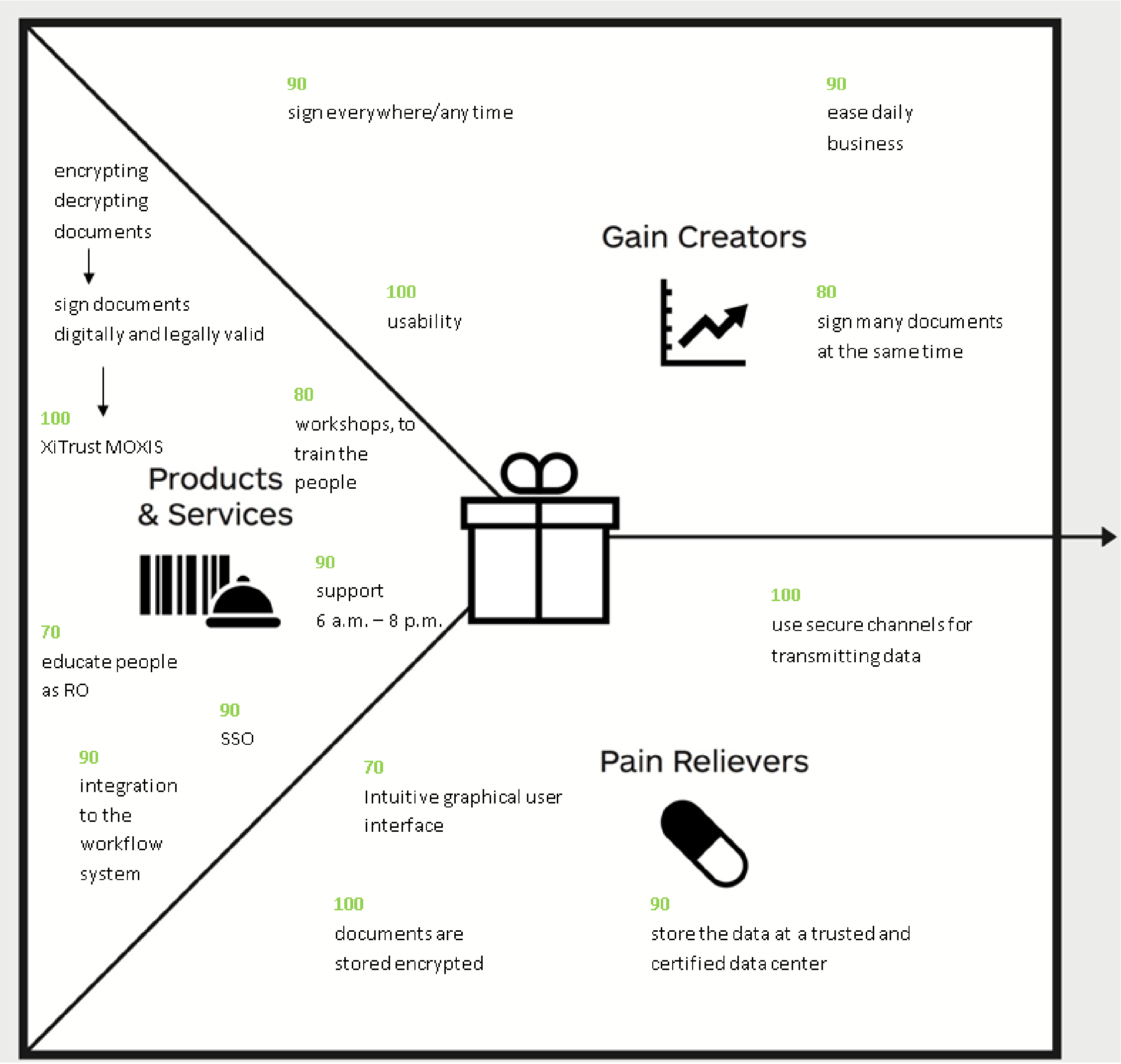

Figure 22.: The value map of *XiTrust* for the doctors (own illustration based on Osterwalder et al. (2014))

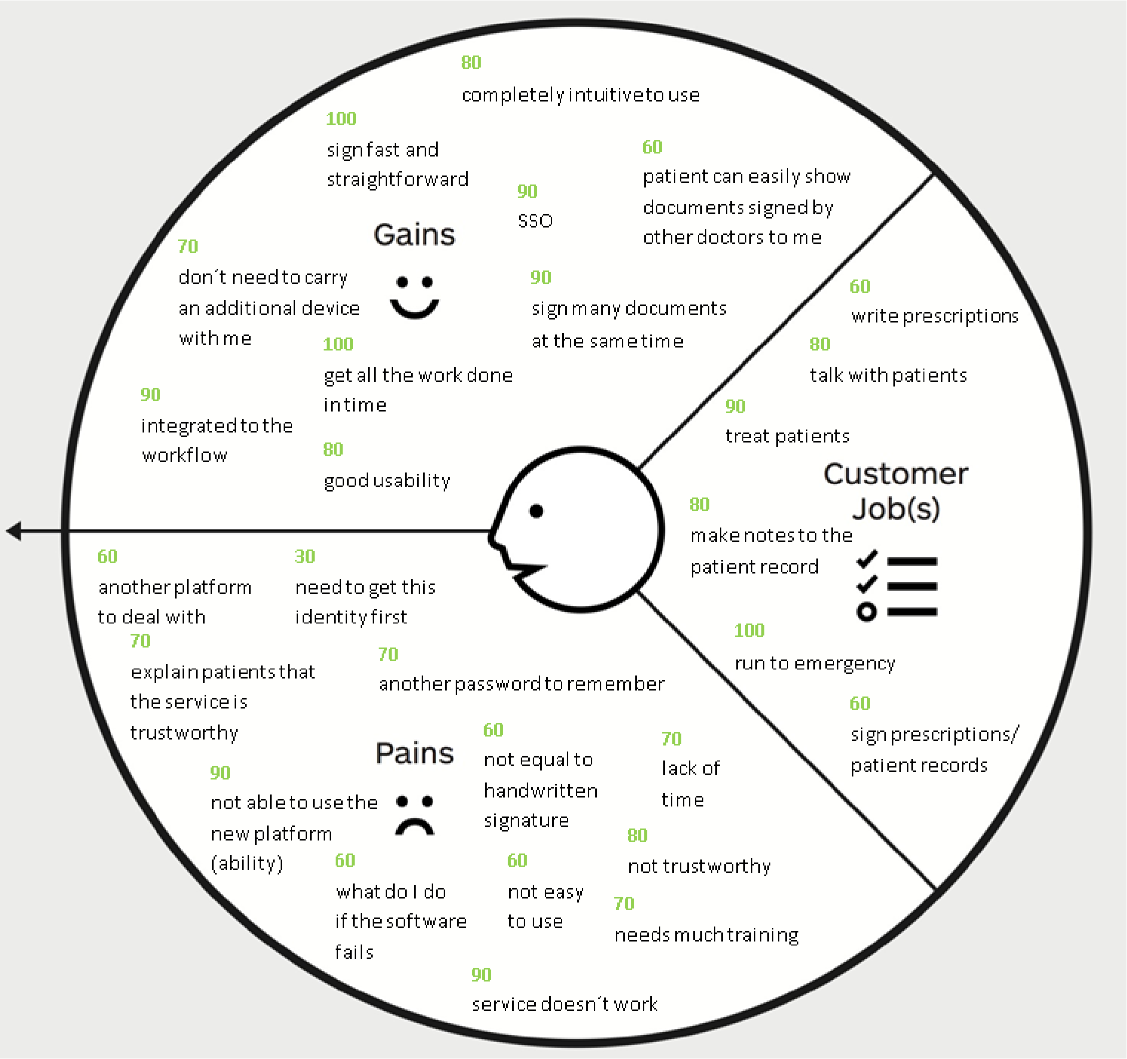
Gains
80
completely intuitive to use
100
sign fast and straightforward
90
SSO
60
patient can easily show documents signed by other doctors to me
70
don´t need to carry an additional device with me
90
sign many documents at the same time
100
get all the work done in time
90
integrated to the workflow
80
good usability
Customer Job(s)
60
write prescriptions
80
talk with patients
90
treat patients
80
make notes to the patient record
100
run to emergency
60
sign prescriptions/ patient records
Pains
60
another platform to deal with
30
need to get this identity first
70
explain patients that the service is trustworthy
70
another password to remember
60
not equal to handwritten signature
70
lack of time
90
not able to use the new platform (ability)
80
not trustworthy
60
what do I do if the software fails
60
not easy to use
70
needs much training
90
service doesn´t work

Figure 23.: The customer profile for the doctors (own illustration based on Osterwalder et al. (2014))

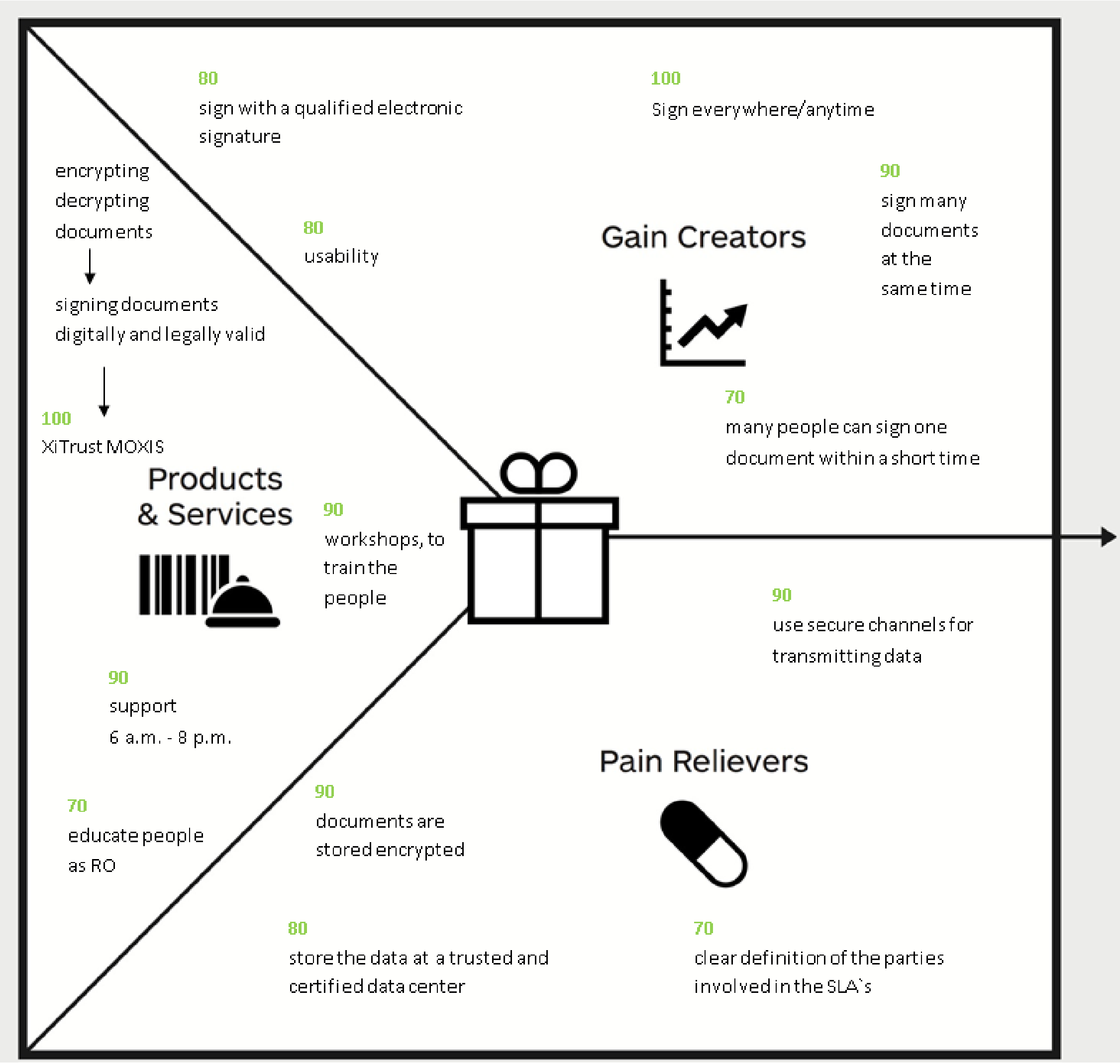
80
sign with a qualified electronic signature
100
Sign everywhere/anytime
encrypting decrypting documents
signing documents digitally and legally valid
100
XiTrust MOXIS
80
usability
90
sign many documents at the same time
Gain Creators
70
many people can sign one document within a short time
Products & Services
90
workshops, to train the people
90
use secure channels for transmitting data
90
support 6 a.m. - 8 p.m.
Pain Relievers
70
educate people as RO
90
documents are stored encrypted
80
store the data at a trusted and certified data center
70
clear definition of the parties involved in the SLA`s

Figure 24.: The value map of *XiTrust* for the patients (own illustration based on Osterwalder et al. (2014))

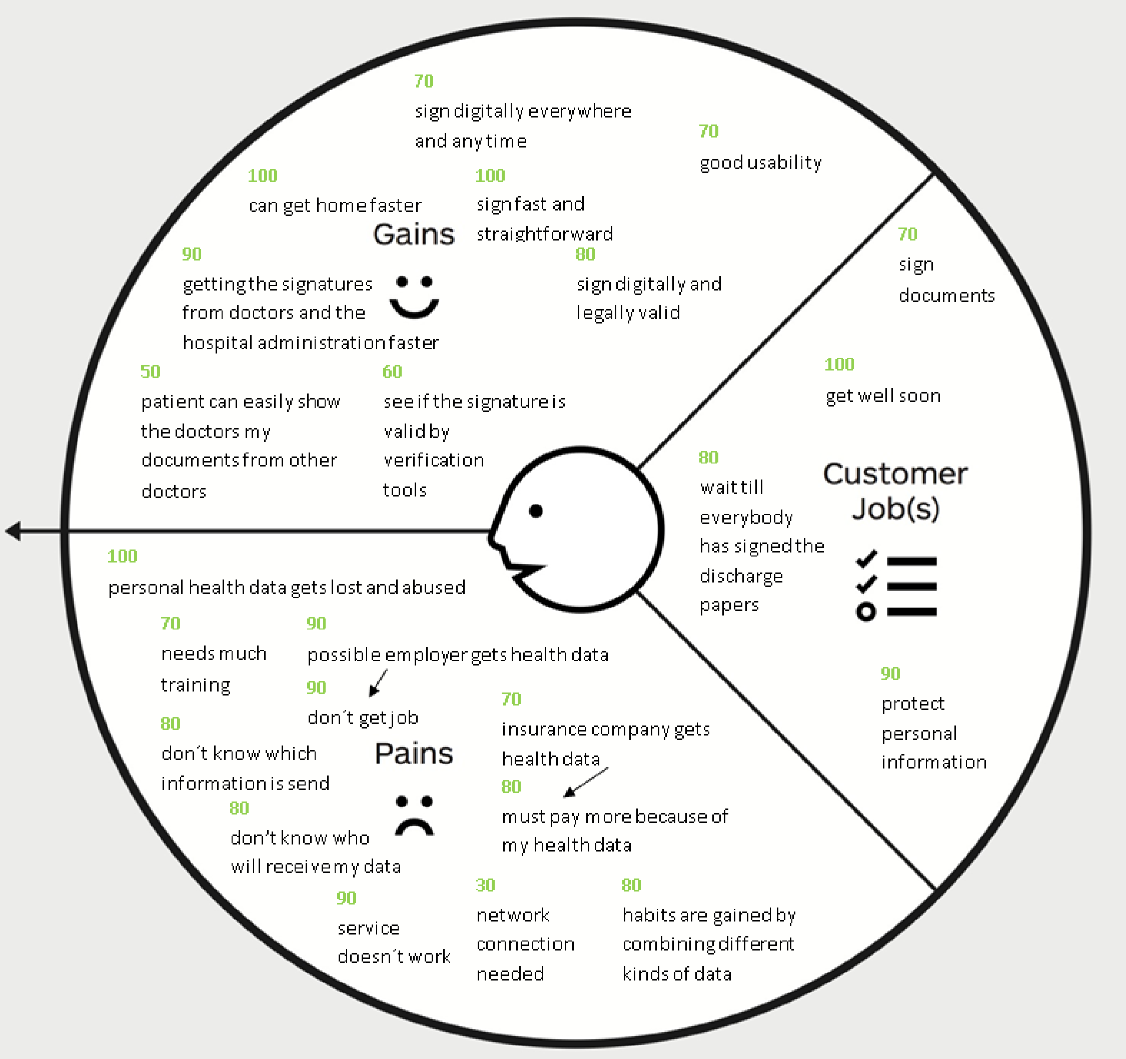
70
sign digitally everywhere and any time
70
good usability
100
can get home faster
100
sign fast and straightforward
Gains
90
getting the signatures from doctors and the hospital administration faster
80
sign digitally and legally valid
70
sign documents
50
patient can easily show the doctors my documents from other doctors
60
see if the signature is valid by verification tools
100
get well soon
80
wait till everybody has signed the discharge papers
Customer Job(s)
100
personal health data gets lost and abused
70
needs much training
90
possible employer gets health data
90
don´t get job
90
protect personal information
80
don´t know which information is send
Pains
70
insurance company gets health data
80
must pay more because of my health data
80
don't know who will receive my data
90
service doesn´t work
30
network connection needed
80
habits are gained by combining different kinds of data

Figure 25.: The customer profile for the patients (own illustration based on Osterwalder et al. (2014))

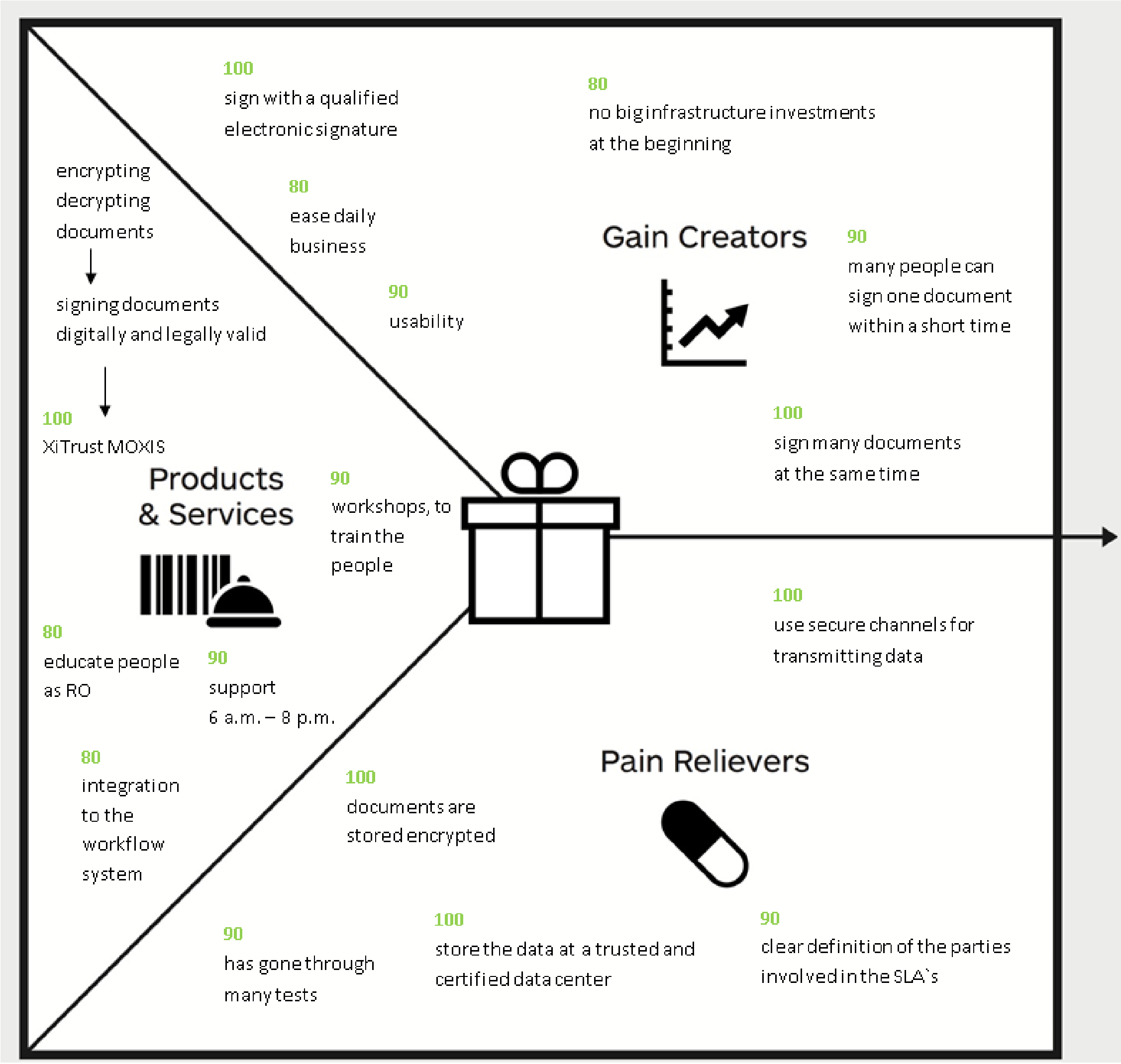
100
sign with a qualified electronic signature
80
no big infrastructure investments at the beginning
encrypting decrypting documents
signing documents digitally and legally valid
80
ease daily business
Gain Creators
90
many people can sign one document within a short time
90
usability
100
XiTrust MOXIS
100
sign many documents at the same time
Products & Services
90
workshops, to train the people
100
use secure channels for transmitting data
80
educate people as RO
90
support 6 a.m. – 8 p.m.
80
integration to the workflow system
Pain Relievers
100
documents are stored encrypted
90
has gone through many tests
100
store the data at a trusted and certified data center
90
clear definition of the parties involved in the SLA`s

Figure 26.: The value map of *XiTrust* for the hospital administrations (own illustration based on Osterwalder et al. (2014))

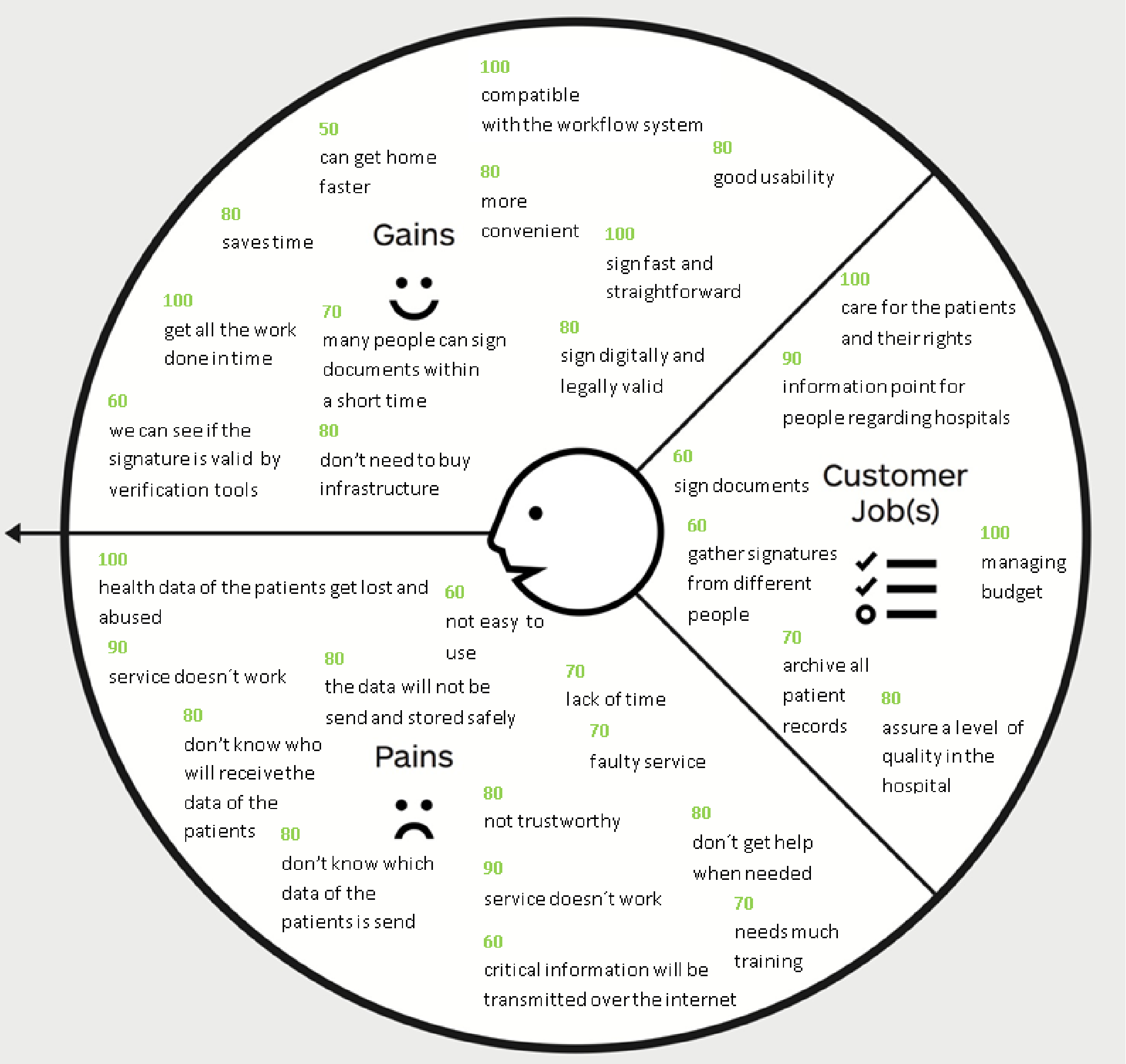

Figure 27.: The customer profile for the hospital administration (own illustration based on Osterwalder et al. (2014))

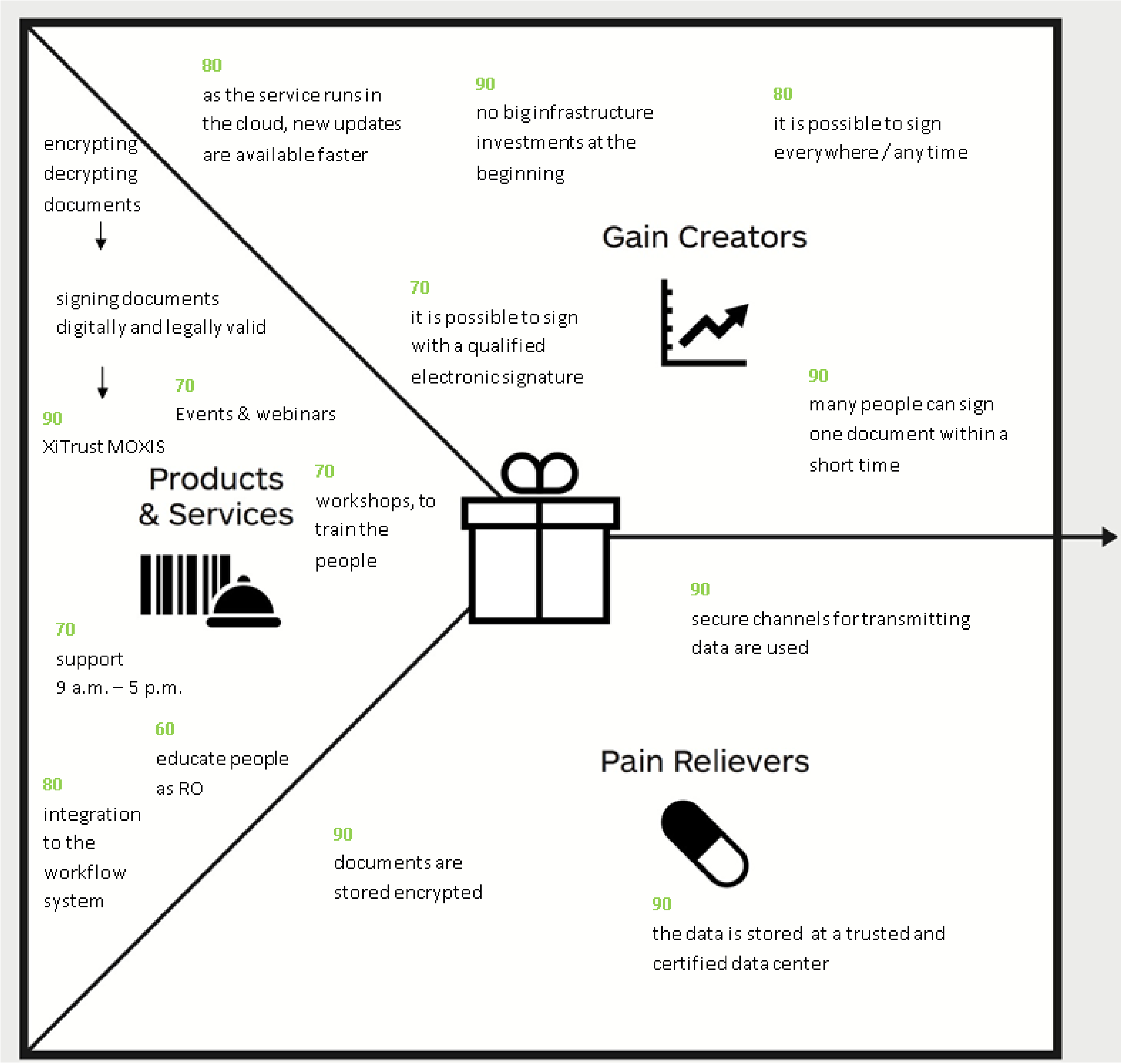
80
as the service runs in the cloud, new updates are available faster
90
no big infrastructure investments at the beginning
80
it is possible to sign everywhere / any time
encrypting decrypting documents
Gain Creators
signing documents digitally and legally valid
70
it is possible to sign with a qualified electronic signature
70
Events & webinars
90
XiTrust MOXIS
90
many people can sign one document within a short time
Products & Services
70
workshops, to train the people
90
secure channels for transmitting data are used
70
support
9 a.m. – 5 p.m.
60
educate people as RO
Pain Relievers
80
integration to the workflow system
90
documents are stored encrypted
90
the data is stored at a trusted and certified data center

Figure 28.: The value map of *XiTrust* for the decision makers (own illustration based on Osterwalder et al. (2014))

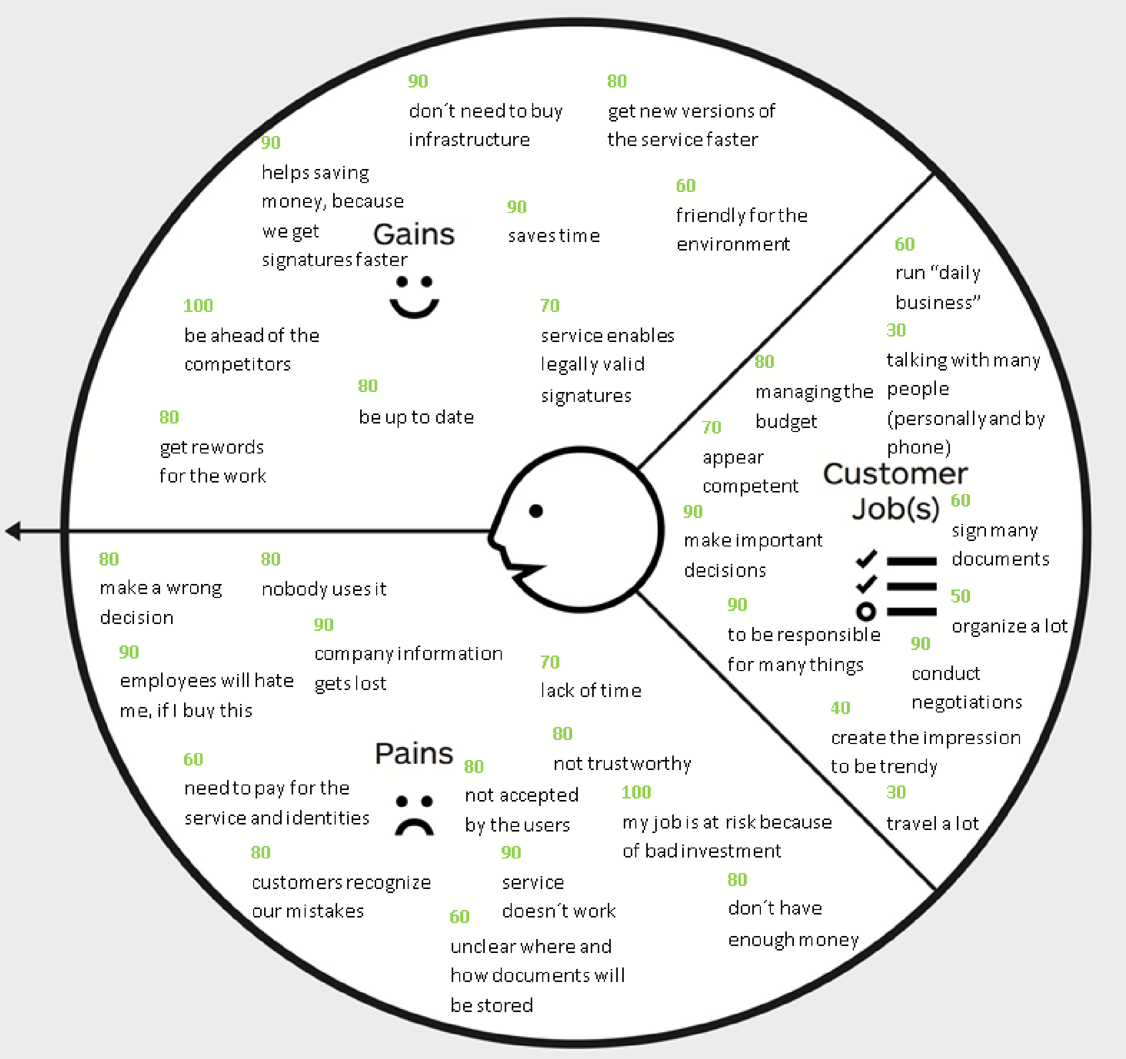
Gains
90
don´t need to buy infrastructure
80
get new versions of the service faster
90
helps saving money, because we get signatures faster
90
saves time
60
friendly for the environment
100
be ahead of the competitors
70
service enables legally valid signatures
80
be up to date
80
get rewords for the work
Customer Job(s)
60
run "daily business"
30
talking with many people (personally and by phone)
80
managing the budget
70
appear competent
90
make important decisions
60
sign many documents
50
organize a lot
90
to be responsible for many things
90
conduct negotiations
40
create the impression to be trendy
30
travel a lot
Pains
80
make a wrong decision
80
nobody uses it
90
company information gets lost
90
employees will hate me, if I buy this
70
lack of time
80
not trustworthy
60
need to pay for the service and identities
80
not accepted by the users
100
my job is at risk because of bad investment
80
customers recognize our mistakes
90
service doesn´t work
80
don´t have enough money
60
unclear where and how documents will be stored

Figure 29.: The customer profile for the decision makers (own illustration based on Osterwalder et al. (2014))

B. Results from Expert Interviews

General Inquiry

1. In your organization, (what means do you use) how do you authenticate documents/ data physically and or digitally? [1]
   GL: Physically: Handwritten signature; Digitally: electronic signature
   AS: Physically: Handwritten signature; Digitally: electronic signature
   TL: Mainly digitally signed with the Austrian citizen card but also with the mobile phone signature.
   CM: Nothing is used.

2. Do you share information with parties outside your organization? How?
   GL: Yes, via e-mail with a server signature, if persons outside the company need to sign something *XiTrust MOXIS* is used.
   AS: Yes, via e-mail.
   TL: Yes, mainly digitally and if the information needs to be authenticated, a digital signature will be provided.
   CM: Yes, we grant people access to our infrastructure with so called external accounts. Some people probably use Dropbox unofficially. We are thinking of an *ownCloud* solution, which should be for all Austrian universities and then all the data could be shared via this platform.

3. Do you use Cloud Services? Why? Which ones?
   GL: Restricted, mobile phone signature, CRM and Office365. The reason why we use cloud services is the cost-effectiveness.
   AS: No, because we are a public institution, most likely private cloud.
   TL: Few, only to store some data.
   CM: You could say yes because we use SAP. We have a cloud like structure on our own because of a virtualization structure which is distributed over two computation sites (private cloud). External cloud services are not used but unofficially maybe Dropbox, OneDrive, GoogleDrive.

4. What systems do you use for authentication/verification? Can you give a short description?
   GL: In-house: PKI via VPN accesses. The certificates are from external trust centers, and we use the mobile phone signature.
   AS: Adobe Reader and RTR Website (Rundfunk & Telekom Regulierungs-GmbH)

[1] The interview questions of this interview originate from (Alaqra et al., 2015)

TL: Citizen card & mobile phone signature to sign digitally and for the local access system username and password, to check signatures the RTR tool or the local testing system which is the same as that from the RTR.
CM: Active Directory, LDAP

a) What are the perceived pros and cons of the system?
GL: Pro: in-house pki: own control over the certificate infrastructure this works only for internal processes; External certificates more expensive and less flexible; mobile phone signature: high quality and easy to register
AS: Adobe Reader: Very comfortable. RTR Website: Not integrated.
TL: Pro RTR: Officially recognized verification service in Austria and if you are a bit familiar with the service it is easy to use. Especially for a Austrian company very practically because all Austrian specific certificates are deposited there. Checking the certificate chain is easier than with Adobe Reader because the newest certificates are only deposited in the newest version. Con: Bad user guidance
CM: Pro: That identity management is regulated within the company Con: None

b) Is it considered private/secure? Is it protected against unauthorized users?
GL: Yes, it is considered private and secure. Yes, it is protected against unauthorized users.
AS: Adobe Reader: Yes, local. RTR website: less secure
TL: Yes, they are considered private and secure. Yes, it is protected against unauthorized users.
CM: Yes, they are considered private and secure. Yes, it is protected against unauthorized users.

c) From your experience have there been any incidents regarding security/privacy? **GL:** No incidents
AS: No incidents
TL: As we develop these systems on our own there have been small incidents where things needed to be corrected but as far as I know they did not affect the system when it was running at the customer.
CM: No incidents

5. What actors are involved in the process, and what levels of authority are they given? **GL:** Everybody in the company but not everybody has the same rights
AS: Everybody in the company
TL: If it is just an internal document only the concerned employee signs. If the document will leave the company, the superior of the concerned employee needs to sign; Level of authority: internal: regulated with username & password; external: regulated with the citizen card
CM: Everybody in the company

Health Care Use Case

Description
Consider a case, where a patient has a smart phone training application that uses the sensors on the phone/wearable device to monitor and collect personal data of the patient. The patient would like to share only activity progress information of the data collected by the application.

1. Do you see the benefit of this case (providing applied functions data instead of raw data)? Why?
   GL: One benefit is that I know which information are passed on because it feels better if I know who receives the information
   CM: Yes, because the recipient of the information does not need to get all the information.

2. What similar functions can you foresee in your organization? Examples?
   GL: None
   CM: For example for security attacks where you are interested in an attack pattern in order to protect your system, what we already do.

E-Government Use Case

Description
Consider a case where a forest fire occurs, and the government would want to release a report about this incident that includes personal information, e.g. about victims or rescue workers, and potentially other classified information (all signed) regarding the cause and procedure to the public, but would want to anonymize all personal information such as, names of rescue workers, victims and/or other people involved.

1. In your opinion, is the report released that was viewed by the public? Is it still verified/authentic i.e., is the original signature still valid? Why/why not?
   AS: Yes, if the person who created the report and the person who changed the report are the same.
   TL: Technically, it is not valid because if the report contained originally all the data, then it was signed and then data was removed entails that the signature is broken. The original is also not valid because afterwards, I cannot verify if it was valid before the changes were made.

   a) Would you trust claims that the signatures will still be valid for the document after all personal information has been „blacked-out“?
      AS: Only if it is resigned after things have been blacked-out.
      TL: I would say that it is valid if a process would exist that can afterwards state that the report has been valid before things were blacked-out.

2. Are there similar examples/cases in your organization, where parts of a document are

modified/edited out, while validity for the unmodified parts should be maintained?
AS: No
TL: There exist a lot of cases where we would need it but it is not practically realized yet. The functionality is desired!

a) How does your system handle modifications?
AS: -
TL: We have prototypes of this kind of system so the answer is referred to these prototypes. Modifications are handled with blank digital signatures.

b) How does your system guarantee that modified documents will have a valid signature?
AS: -
TL: Through a cryptographic signature process. Basic idea: A template where every field that can be blacked-out has two properties either blacked-out or the actual value. The template is signed so that the validity of the template self can be verified and then an instance is created either with the values or they are blacked-out and signed again.

3. From your experience, what other signature related issues/challenges can you share?
AS: That old signatures lost their validity because some information has been added afterwards.
TL: None

Requirements Follow Up

1. In your perspective, for a system dealing with digital signatures, what are the fundamental requirements? What does the system need to fulfill in order to be considered trustworthy? Secure? Private? Authentic?
GL: The mobile phone signature for example, fulfills these requirements perfectly.
AS: The system should operate locally and if data is send outside, that it is clear, which data is send.
TL: The system should be build upon a trustworthy base, use up-to-date libraries and it should be implemented from persons who have not just implementing knowledge but also knowledge regarding cryptographic processes. Further, a trustworthy company who manages the certificates is needed and that the system is maintained correctly and implemented correctly regarding security and privacy directives.
CM: Through falsification (exists a case where the system did not work secure…). Complete Transparency, compliant with the law and the person also needs to trust the system.

2. What are your general concerns when it comes to security/privacy in cloud services (outsourcing)?
GL: To communicate, to the customer that the cloud is really secure, data is kept private and make it clear that he/she can trust the cloud service.
AS: Legal concerns, information privacy, public cloud: Where is the information stored and

can we do something legally if incidents would happen, will we be informed if data is passed on or any incidents happened?
TL: That the cloud provider is very curious about user data and that he/she wants to analyze user and their data and also use them for other purposes.
CM: That data is misused (data mining). Therefore the data at the service provider should be stored in a way that only the customer can use the data.

3. What are security requirements for your organization for using cloud services (outsourcing)?
   GL: In the end we have to trust a third party and an institution needs to make IT security audits there. Checks that verify if the third party fulfills the data protection directives should be made, the institution which does the audits should have access to the stored data there and also the employees in the third party should be checked.
   AS: No cloud services are used.
   TL: Cloud services are not used a lot and if just for documents with a very low level of security (GoogleDocs).
   CM: Data must be stored securely, complete transparency (how is data stored, encryption).

4. Would you trust that contractual agreements, certification and auditing schemes will be sufficient for ensuring security for data outsourced to the cloud? Or would you put more trust on crypto-based security solutions?
   GL: We use crypto-based solutions everywhere, where it is possible to use but both is necessary cryptography & contractual agreement. The importance of the documents plays also a role.
   AS: At any rate, crypto based. End to end encryption. Hardware based encryption till RAM.
   TL: More trust on crypto-based solutions. The cloud service provider should not get the data, therefore data should be stored encrypted and it should only for the user be possible to decrypt the data.
   CM: More trust on crypto-based solutions, because a contractual agreement can be broken.

Interview

Part A: General Inquiry

1.	In your organization, (what means do you use) how do you authenticate documents/data physically and or digitally?
2.	Do you share information with parities outside your organization? How?
3.	Do you use Cloud Services? Why? Which ones?
4.	What systems do you use for authentication/verification? Can you give a short description?
4.1.	What are the perceived pros and cons of the system?
4.2.	Is it considered private/secure? Is it protected against unauthorized users?
4.3.	From your experience has there been any incidents regarding security/privacy?
5.	What actors are involved in the process, and what levels of authority are they given?

Table 1: Results for Part A (General Inquiry)

A	1.	2.	3.	4.	4.1.	4.2.	4.3.	5.	-	-
	a. Physical documents authentication means b. Digital documents authentication means	a. Sharing information outside organization b. Means	a. Response b. Reason C. Examples	a. System used by the organization for authenticating documents/data	a. Pros of the system b. Cons of the system	a. Response b. Extra info.	List of Incidents jeopardizing security /privacy	List of actors involved in the system and their level of authority	List of additional information points	List of comments of the interviewers

Part B: Case scenarios

Option i: Health care part (1/2)

Description

Consider a case, where a patient goes to the doctor for a routine check-up and takes an extensive blood test. The blood test is taken by the doctor's nurse and the results are uploaded to the portal and are digitally signed by the nurse. The doctor has access to the complete blood test results.

NEXT>> the patient visits a dietitian, who requires few specific fields of the blood test. The patient doesn't want to reveal all fields from the extensive blood test. So the patient selects the mandatory fields from the extensive blood test for the dietitian to see and "blacks-out" the other fields.

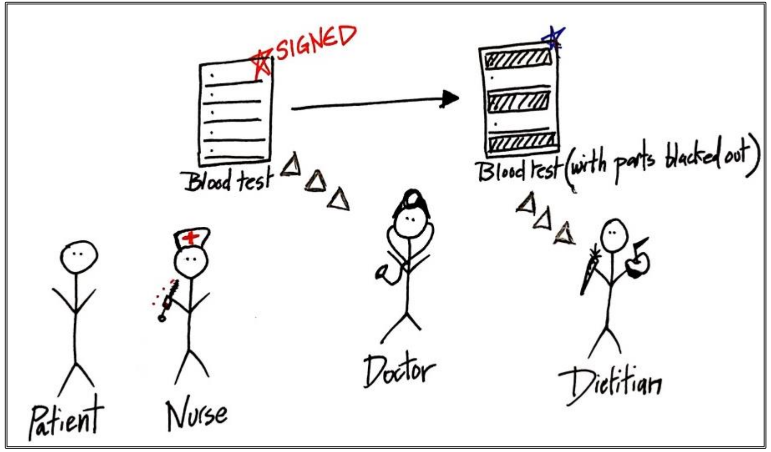

Figure 1: blood test use case

Alternative similar case:

Consider a case, where a patient goes to the doctor for a routine check-up and takes an extensive blood test. The blood test results and diagnosis report are uploaded to the portal and are digitally signed by the doctor. The doctor has access to the complete blood test results.

NEXT>> the patient wants a second opinion from another doctor on her results. The patient doesn't want to reveal the diagnosis fields from the report. So the patient selects the blood test results for the second doctor to see and "blacks-out" the diagnosis fields.

1. In your opinion, is the blood test that was viewed by the dietitian still verified/authentic, i.e. is the nurse’s signature still valid? Why/why not?

    1.1. Would you trust claims that signatures for parts of the document are still valid?

2. Are there similar examples/cases in your organization, where parts of a document are modified/edited out?

    2.1. How does your system handle modifications?

    2.2. How does your system guarantee that modified documents will have a valid signature?

3. From your experience, what other signature related issues/incidents can you share?

Option i: Health care part (2/2)

Description

Consider a case, where a patient has a smart phone training application that uses the sensors on the phone/wearable device to monitor and collect personal data of the patient. The patient would like to share only activity progress information of the data collected by the application.

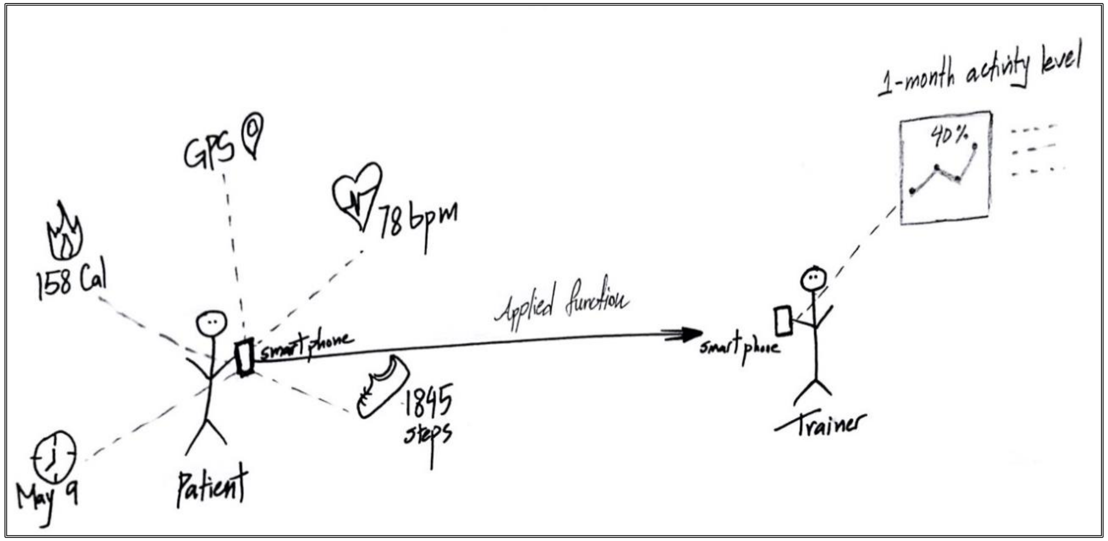

Figure 2: monitor application use case

4. Do you see the benefit of this case (providing applied functions data instead of raw data)? Why?

5. What similar functions can you foresee in your organization? Examples?

Table 2: Results from Part B.i (Health care)

B.i	1.	1.1.	2.	2.1.	2.2.	3.	4.	5.	-	-
	a. Response/ opinion b. Reasons	a. Response b. Extra info.	List of similar examples/cases	Means of handling modifications	Means of validity verification	List of experiences/ issues/incidents	a. Response b. Reason c. Extra info.	a. List of similar functions b. Examples	List of additional information points	List of comments of the interviewers

Option iii: E-government part (1/2)

Description

For disaster recovery and backup purposes, IT providers of governmental institutions split their databases into multiple parts (shares) that are stored at independent cloud providers. Consider a case where a disaster occurs, and a potential data loss is at risk. To reconstruct data, only a predefined subset of shares stored at different cloud providers would be required, e.g., 4 shares out of 7.

1. Do you have disaster protection mechanisms? What are they?

    1.1. Do they protect against data loss?

2. Do you have any data recovery mechanisms? What are they? How does it address confidentiality of backups?

3. Do you see benefits in such solutions? Would you use such backup/data-sharing setup? Why/why not?

Option iii: E-government part (2/2)

Description

Consider a case where a forest fire occurs, and the government would want to release a report about this incident that includes personal information, e.g. about victims or rescue workers, and potentially other classified information (all signed) regarding the cause and procedure to the public, but would want to anonymize all personal information such as, names of rescue workers, victims and/or other people involved.

4. In your opinion, is the report released that was viewed by the public is still verified/authentic i.e., is the original signature still valid? Why/why not?
    - 4.1. Would you trust claims that the signatures will still be valid for the document after all personal information has been "blacked-out"?
5. Are there similar examples/cases in your organization, where parts of a document are modified/edited out, while validity for the unmodified parts should be maintained?
    - 5.1. How does your system handle modifications?
    - 5.2. How does your system guarantee that modified documents will have a valid signature?
6. From your experience, what other signature related issues/challenges can you share?

Table 3: Results for Part B.iii (E-Government)

B.iii	1.	1.1.	2.	3.	4.	4.1.	5.	5.1.	5.2.	6.	-	-
	a. Response b. mechanisms	Response	a. Response b. Data-recovery mechanisms	a. Response b. Reason	a. Response / opinion b. Reasons	a. Response b. Extra info.	List of similar examples/cases	Means of handling modifications	Means of validity verification	List of experiences/ issues/incidents	List of additional information points	List of comments of the interviewers

Part C: Requirements follow up

1. In your perspective, for a system dealing with digital signatures, what are the fundamental requirements? What does the system need to fulfill in order for it to be considered trustworthy? Secure? Private? Authentic?
2. What are your general concerns when it comes to security/privacy in cloud services (outsourcing)?
3. What are security requirements for your organization for using cloud services (outsourcing)?
4. Would you trust that contractual agreements, certification and auditing schemes will be sufficient for ensuring security for data outsourced to the cloud? Or would you put more trust on crypto-based security solutions?

Table 4: Results for Part C

C	1.	2.	2.	3.	4.	-	-	-
	List of requirement for a. Trust b. Security c. Privacy d. Authenticity	Security concerns in the cloud	Privacy concerns in the cloud	Security requirement in the Cloud	Response	List of additional information points	List of comments of the interviewers	