Aalto University - Department of Communications and Networking

ELEC - E7830 Value Network Design for Internet Services

Case: Initial Authentication Service

27 April 2017

Bhavya Omkarappa, bhavya.omkarappa@aalto.fi, 600824

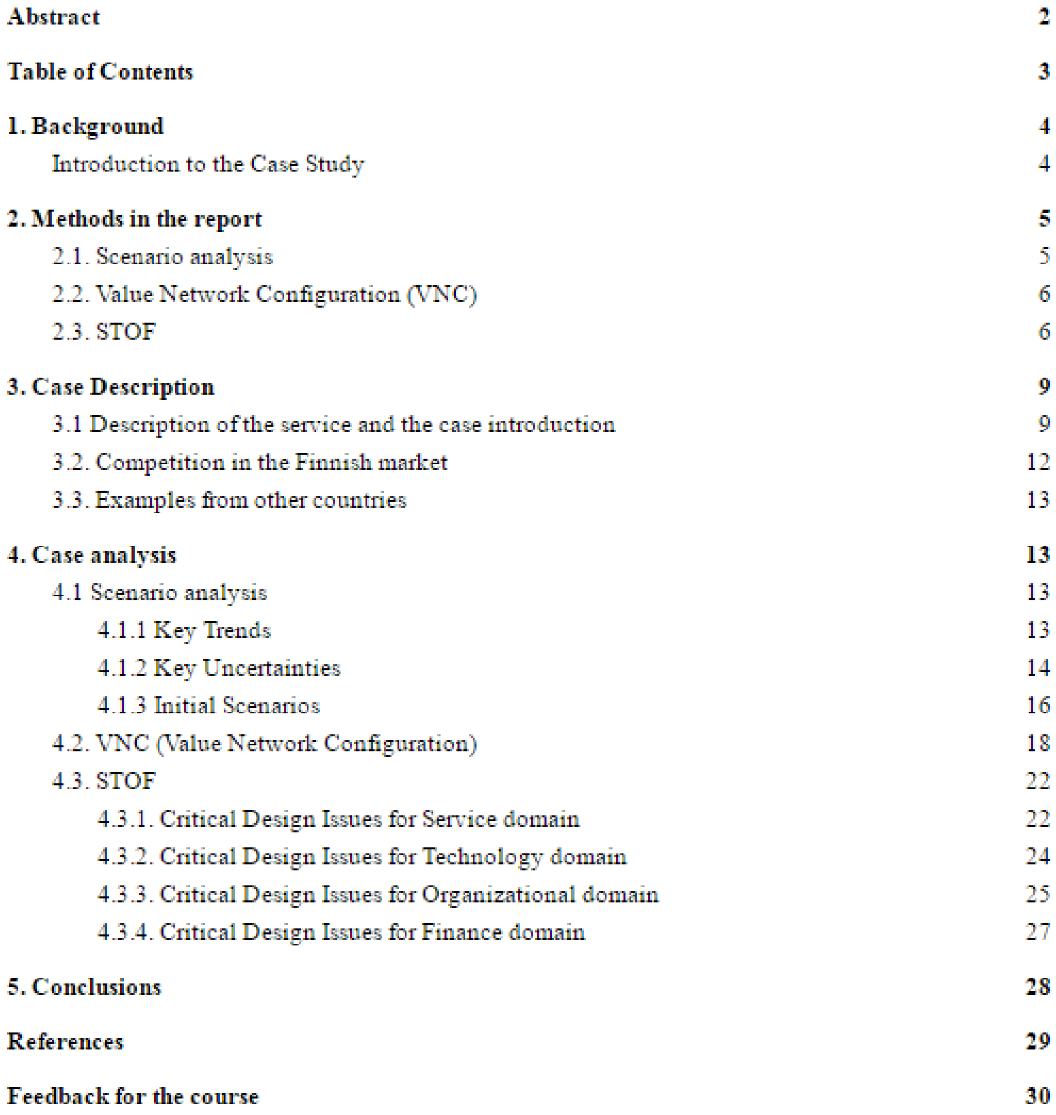
Florian Lalet, florian.lalet@aalto.fi, 621913

Hanna Koponen, hanna.koponen@aalto.fi, 399795

Abstract

Evolving technologies are changing the customer expectations to the services. Since many services are already available in Internet and mobile phones, people are more willing to have more and more services available anywhere and at any time. Banks are also affected by this changing customer expectation. Currently, there is a bank visit needed to get new bank credentials. Banks themselves are more willing to provide services to get bank credentials online or with mobile applications to fulfill customer needs and also to make their work more efficient. Since, there are several security and trust issues to be tackled to be able to provide the bank credentials as mobile or online service. In this report, we are diving in this topic using three different methods. First, Scenario analysis method is used to define and map key uncertainties and trends to create business scenarios. Second, Value Network Configuration method is used to define the service's business and technical structure. The third method, STOF, focuses in critical design issues and critical success factors of the service.

Table of Contents



Abstract **2**

Table of Contents **3**

1. Background **4**
- Introduction to the Case Study 4

2. Methods in the report **5**
- 2.1. Scenario analysis 5
- 2.2. Value Network Configuration (VNC) 6
- 2.3. STOF 6

3. Case Description **9**
- 3.1 Description of the service and the case introduction 9
- 3.2. Competition in the Finnish market 12
- 3.3. Examples from other countries 13

4. Case analysis **13**
- 4.1 Scenario analysis 13
  - 4.1.1 Key Trends 13
  - 4.1.2 Key Uncertainties 14
  - 4.1.3 Initial Scenarios 16
- 4.2. VNC (Value Network Configuration) 18
- 4.3. STOF 22
  - 4.3.1. Critical Design Issues for Service domain 22
  - 4.3.2. Critical Design Issues for Technology domain 24
  - 4.3.3. Critical Design Issues for Organizational domain 25
  - 4.3.4. Critical Design Issues for Finance domain 27

5. Conclusions **28**

References **29**

Feedback for the course **30**

1. Background

This document is a final report made by the authors of Aalto University course page ELEC-E7830 Value Network Design for Internet Services held during Spring 2017, concentrating on understanding about the theory and design processes of value networks in Internet in the design cases on the field. Our case study was with S-Pankki Initial Authentication Service. This included close collaboration with the bank and to derive the value network design for the case. The course included 3 presentations related to various steps towards deriving the value network design for the case and a final presentation which was inclusive of all. and these presentations were used as a basis for this final report. In addition to including all relevant information from these presentations, some additional information discovered from the bank representative and also from various sources. The feedback from the opponent's team, the course assistant and the professor is also incorporated in the final report.

After this opening section of background information and introduction, the report then describes the methods implemented for the value network design for the case study which includes scenario planning, value network analysis and STOF model. The later sections has the Critical design issues with respect to service, technology, organizational and finance domain of the case study. The report is then finalized with final conclusions about the topic and feedback for coursework.

Introduction to the Case Study

The impressive number ways to open an account and the many factors that are influencing its evolution make it clear that no one technology or channel will define the future of account opening. For potential new customers, mobile account opening is an initial proving ground for a bank’s or credit union’s digital capabilities. (‘Understanding Mobile Account Opening Options’,2014). There are a lot of improvements for the future banking.

S-Pankki is the bank of the S-Group, a Finnish retailing cooperative organisation. S-Bank is the first so called supermarket bank in Finland. Changes in legislation about personal accounts at co-operatives made them uncompetitive, such that founding an entirely new bank was actually easier than keeping the personal accounts as co-operative funds. (S-Pankki, 2014).

The case study of Initial Authentication Service mainly aimed at improving the current procedure of opening a bank account for a new customer. To eliminate the need of the customer to visit the bank and open an account is the focus of this case. This is done by using digitalised methods which includes a mobile application and verification procedures. The bank S-Pankki aims to provide such kind of a feature to the customers in future. In this report we look at the present procedure and analyse different aspects of the solutions. We have considered the business and technical details for the proposed solution.

2. Methods in the report

In this section we describe the methods that are used in the section 3 to analyze the S-Pankki initial authentication service case. The methods are scenario analysis, value network configuration and STOF.

2.1. Scenario analysis

By identifying basic trends and uncertainties, we can construct a series of scenarios that will help to compensate for the usual errors in decision making. Scenario Planning simplifies the avalanche of data into a limited number of possible states. Scenario planning attempts to compensate for two common errors in decision making which are unprediction and overprediction of change. (Schoemaker, 1995)

The process for developing the scenarios are broken down into simpler methods.

1. Define the scope
2. Identify the major stakeholders
3. Identify basic trends
4. Identify the key uncertainties

5. Constructing the initial scenario themes
6. Check for consistency and plausibility
7. Develop Learning Scenarios
8. Identify Research needs
9. Develop Quantitative models
10. Evolve toward Decision Scenarios (Schoemaker, 1995)

Scenarios describe generically different futures rather than variations on one theme. (Schoemaker, 1995). The scenarios derived using the above steps will be used as the basis for further analysis with the Value network configurations and the STOF model. The last few steps of the scenario planning of developing quantitative models were not carried out.

2.2. Value Network Configuration (VNC)

Value network can be understood as a set of interlinked business actors and technical resources that work together to create business and economic value through services and products. The VNC method consist of three steps. First step is analyzing the roles, their value logic and the drivers for value logic importance. Second step is drawing the VNC pictures that include business interfaces, technical interfaces, actors, technical components and business roles. (Heikkinen et al, 2010)

2.3. STOF

STOF model provides a holistic view on product’s or service’s business model. It consist of four domains: Service domain, Technology domain, Organizational domain and Finance domain. These domains together provide a descriptive framework for the design of business models. Customer value of the product or service has an important role in the model. (Bouwman et al. 2008). STOF model is shown as a descriptive picture below.

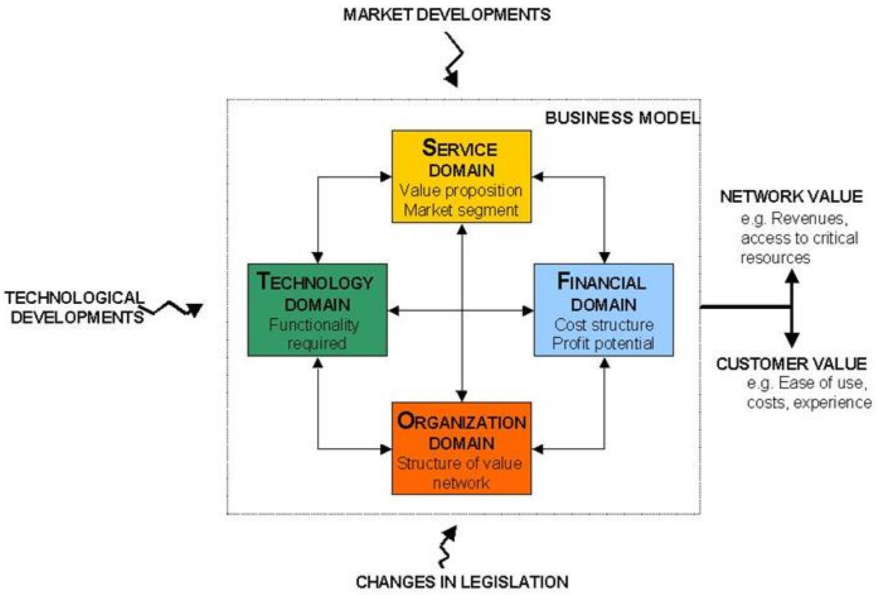


Figure 1. The STOF model in general (Bouwman et al., 2008, used with permission)

Service domain is the starting point of STOF model. The main goal in the service domain is to define the customer value of the service. Target customer group, branding, customer retention and trust are defined in service domain. (Bouwman et al)

Service domain creates and specifies the requirements that are combined into technical architecture in technology domain. User authentication, management of user profiles and security are aspects of the technology domain. (Bouwman et al, 2008)

Organizational domain analyses issues related to resources, capabilities, marketing and finance. It includes also defining actors, value network, interactions and strategies and goals, value activities, resources and capabilities. (Bouwman et al. 2008). Organizational domain of STOF has similar things to be defined than there is in VNC model.

The two main issues in financial domain are investment decisions and revenue models. In finance domain cost structure is analyzed and scalability and service bundling is considered. Also pricing of the product/ service, revenue models, including where income is created and what it being paid, are considered in finance domain. Finance design includes investment and cost sources, revenue and risk sources, pricing and financial arrangements. (Bouwman et al, 2008)

The STOF model is analyzed with STOF method. The method helps designers in creating working and feasible business models to create value for the customer. The method consist of four steps: Quick scan, evaluation of critical success factors, specifying critical design issues and making a robustness check. (Bouwman et al. 2008)

Quick scan step includes the aspects from the four domains of STOF model. The aim is to answer basic questions like “Who is the customer?”, “What is the service?”, “Why would someone want to use the service?”, “Which technologies are needed”, “What are the activities, actors and roles in the value network?” and “Will there be enough revenue to compensate efforts, costs and risks”? (Bouwman et al. 2008)

Step 2, evaluation of critical success factors(CSFs), analyzes how well business model satisfies critical success factors for viable business model. It is important that CSF’s are related to the customer value creation. The results of this step are qualitative judgements. (Bouwman et al. 2008)

Step 3 is specification of critical design issues(CDI’s). In this step, selected CDI’s are specified more detailed depending on the CSF evaluation. The process for this follows STOF model domains and the goal is to get all CDI’s balanced. (Bouwman et al. 2008)

Step 4 is robustness check. Since business models evolve during time, robustness check analyzed the business model’s ability to cope the changes. (Bouwman et al. 2008)

3. Case Description

In this chapter, we’ll describe the credential creation process by the bank and provide some examples from the competition in Finnish market. We’ll also provide some examples from other countries.

3.1 Description of the service and the case introduction

To get bank credentials, the customer needs to visit the bank. S-Pankki has defined that to get bank credentials, the customer needs to have bank account in S-Pankki or wide disposition to some else's S-Pankki account. He or she also has to be older than 12 years old and have identification card or passport when visiting the bank. (S-Pankki, 2017)

In Finland, bank credentials are used also identifiers to access public services online. There are e-services available for all the government agencies. Before accessing these services, the customer needs to first visit the bank to get the bank credentials. It is important that bank credentials are personal to access the government e-services. Suomi.fi site guides that the customer needs to make sure that no one else has access to citizens ID, passport or keycode list. Security is important when using government e-services. (Suomi.fi, 2017)

Next, we will present the service, our problem we have worked on it. The problem is about the initial authentication for opening a bank account, or for getting a bank credential. We have this issue : *Is there other opportunities to get a bank credentials than visit bank office for a person who doesn’t have any previous back credentials?* To understand the case in the first place we need to explain the current process that is shown in the next picture.

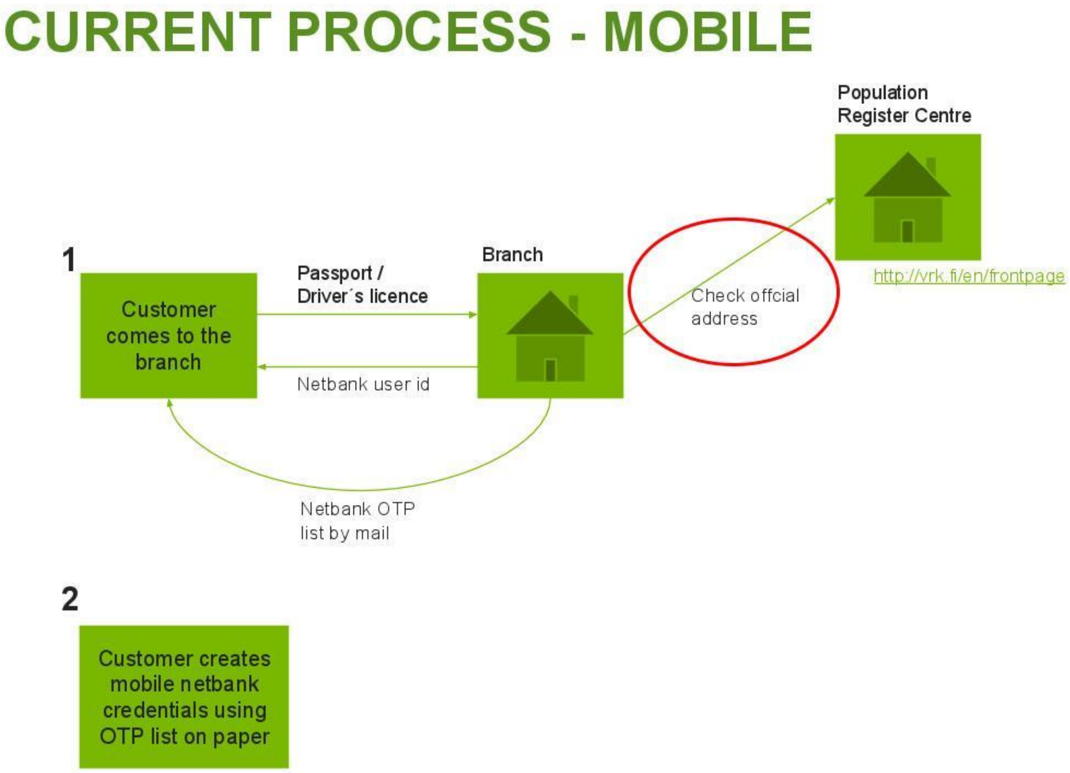

CURRENT PROCESS - MOBILE
1
Customer comes to the branch
Passport / Driver´s licence
Netbank user id
Branch
Check offcial address
Population Register Centre
http://vrk.fi/en/frontpage
Netbank OTP list by mail
2
Customer creates mobile netbank credentials using OTP list on paper

Figure 2 : Correct S-Pankki credential creation process (From Carl-Edvard Holmberg) Used with permission.

In this current process, the customer bank have to visit a branch of the bank (S-pankki in our case). The customer come with an ID and give his address. the bank will check from the population register centre if the address is valid. Finally the customer create mobile netbank credentials by using password sent by mail to your accommodation.

We want to change this process to have an easier way for authentication to avoid the visit in the branch. In this purpose, we will use the smartphone to have a faster way, less requirements. For instance, you could be in your flat, or be abroad while open a new bank account.

3.2. Competition in the Finnish market

There are 238 banks in Finland (Rahoitusvakausvirasto, 2017). Most of the bank work in co-operation or are part of the bigger bank chain. Two biggest banks in Finland are Nordea and OP-Pohjola, one middle size bak is Danske Bank. (Taloussanomat.fi, 2017). To get overall how different banks create customer’s bank credentials, we chose these three to be checked. What we noticed is that all Nordea (Nordea.fi, 2017), OP-Pohjola (OP.fi, 2017) and Danske Bank (Danskebank.fi, 2017) want the customer to visit the bank with ID card or passport before they can get bank credentials. This means that none of these banks have yet found a secure enough solution to identify the customer without visiting the bank. It still can be that all the banks are looking actively or not actively solution for the dilemma.

Other competitors for identification can be the government, who could do the identification for the user and also provide credentials for public services. Bank's main business is banking services, not ID credentials that can be used in other services as well. Now the banks are responsible to provide good enough identification for the public services as well, but it could be government who was responsible for that.

If banks would still provide the credentials that are used for identification in different public services, the initial authentication service (is now visit the bank with ID card) could be replaced by identification of other service provider. One solution could be that some start-up company creates a solution for biometric etc. identification that is combined with passport for example to create a high level identification. In this case, other third parties are somehow competitors for the bank.

3.3. Examples from other countries

To see how the identification is provided in other countries, we chose Sweden, Norway, France, India and Estonia as examples. The usage of bank credentials varies and in some countries the credentials are used only for banking services and in some countries also to government services. Identification to get the credentials is done in the bank office or government office, depending from the country. None of the countries we have as an example provide identification services (initial authentication) to get the credentials online.

In Sweden and Norway common Bank ID is created for users of many banks. Identification to get the common ID is done by the banks in the bank office with passport (Norway) or national ID card (Sweden). (BankID.com, 2017 and BankID.no, 2017). The difference to Finnish market is that the Bank ID in common for users of different banks, while in Finland the credentials are different depending what bank customer the user is.

In Estonia, to use the public services online the bank credentials are not needed. To get unique 11-digit code the customer needs to visit county government in person with personal ID. (Workinestonia.com, 2017). Difference to Finland is that bank credentials are not used for identification to government e-services and the ID for those is provided by government.

In France, it is possible to open a bank account online without visiting the bank. To open this bank account you need to have a previous account in another bank. More precisely, you need to transfer money from a bank account in Europe. Moreover, you have the possibility to open this account without a previous one if your parents have one. In the biometrical domain, some French bank begin to use this for authentication, use voice recognition, or fingerprint to access to your online bank application.

In India to get a bank account, it is usually done by visiting the bank in person along with your original and copies of the identification and address verification documents. Different Bank ID for users of different banks Identification is done by the banks in the bank office with identification proof like the PAN card and the address proof like driving license or the house contract or even the electricity bill of the house you are living in. A recent photograph is also required along with the above mentioned documents.

4. Case analysis

4.1 Scenario analysis

In this section, we analyse the possible scenarios by observing and noting the key trends and the key uncertainties. The Key trends are with respect to the important trends that we have observed in the market and also the technology. The key uncertainties serves as one of the basis for constructing the scenarios. This serves us for further analysis of the value network design and the STOF model for our case study. While we consider the two most key trends and the key uncertainties, we have constructed the initial scenarios which is helpful and influential to the case study of S-Pankki.

4.1.1 Key Trends

The trends that we have observed and considered for the case is as follows.

T1: Growth in mobile service usage

The global mobile economy is currently $1.6 trillion and will reach $2 trillion by 2017.Mobile applications make people more productive and innovative, freeing them from the tether of stationary computers [Darrell M. West, Joshua Bleiberg, 2014]. This trend influences to have new applications in the banking field where we can use these applications in the mobile for the customers to create and manage new accounts, without having to visit the bank to open a new account.

T2: Changing customer expectations in service: people want easy, efficient, anytime and anywhere service

While we observe the consumer’s expectations and their behavior, it is seen from research that the consumers value for time, the service bought for their money which is efficient and also which makes their life easy. The application or the service which is offered to the customer needs to be user friendly and user efficient. The expectations of the customer is changing. This is one of the trend which influences the case study since the evolvement of the solution will be accepted by the customers since the focus is to eliminate the step of the person visit to the bank to open the account.

T3: Migration and studying abroad grows -> more people without previous bank credentials

People migrate to different countries for a lot of reasons. And one of the main reason is for studying for the youth. Foreign born individuals correspond to 2.7% of the population of Finland.['Immigration to Finland', 2016]. When people migrate, there is a requirement to open a bank account. If the person migrate to a different country within Europe, there are new opportunities in banking sector to use the previous credentials of a different European bank to open a new bank account without having to visit the bank.

T4: Electronical development of payment etc. banking related technologies continues growing fast

As we have seen in today's banking sector, there is a lot of improvement in banking which is becoming digitalized. The bank transactions and all the services can be done online. With this trend it is quite optimistic for the new opportunities to even open a bank account through a mobile application.

T5: Cooperation and common databases inside EU provide better translation of personal information

Having common databases which includes personal information and the address of that person is quite useful for many sectors and even for banking.

4.1.2 Key Uncertainties

The key uncertainties which helps us construct the scenarios for the case study are as follows.

U1: Who takes care of the identification: bank or third party company?

When a bank account is opened through a mobile application, the next step for is to do the identification and the verification of the individual. This is a challenge since it is quite critical. The question of who is held responsible for the identification and the verification, whether it is the bank itself or a third party company which can even be the government is an uncertainty which helps us determine the scenarios for this study case.

U2: Can the biometrical identification reach a enough level of security? Do we need one or two level of security check like for example biometric identification and address ID verification.

Identification is a crucial step as it comes along with a lot of risks if it is done incorrectly. The uncertainty of the level of identification increases along with the increase of the complexity of the application to open the bank account. The question if the biometric identification is sufficient or not is something which determines how we construct the scenarios. Or if we need more levels of the security like biometric identification and address ID verification for the initial authentication to open a new bank account.

U3: Can bank trust the third party identification?

If there is a third party who is offering the identification check for the banks for opening an account, there is a question as to how far are they trustworthy.

U4: Is imposing of the requirement for ID card needed even for opening the bank account?

For new international customers, existing international customers, new Finnish customers and the existing Finnish customers, is it mandatory to impose the requirement of an ID card to open the bank account is an uncertainty which determines the scenarios to a new level.

U5: Can the banks trust other banks to provide bank credentials for people who are already customers for other bank?

Is there trust between banks for the identification and address verification for the customers who already have the credentials in other banks. Can these credentials be used to open a new bank account in another bank without undergoing any other procedures for identification and verification.

4.1.3 Initial Scenarios

Among the uncertainties mentioned in the previous section, U1 and U2 are the most relevant to understanding and constructing the scenarios for the case study of S-Pankki. Figure 3 represents the different scenarios built upon considering the uncertainties U1 and U2.

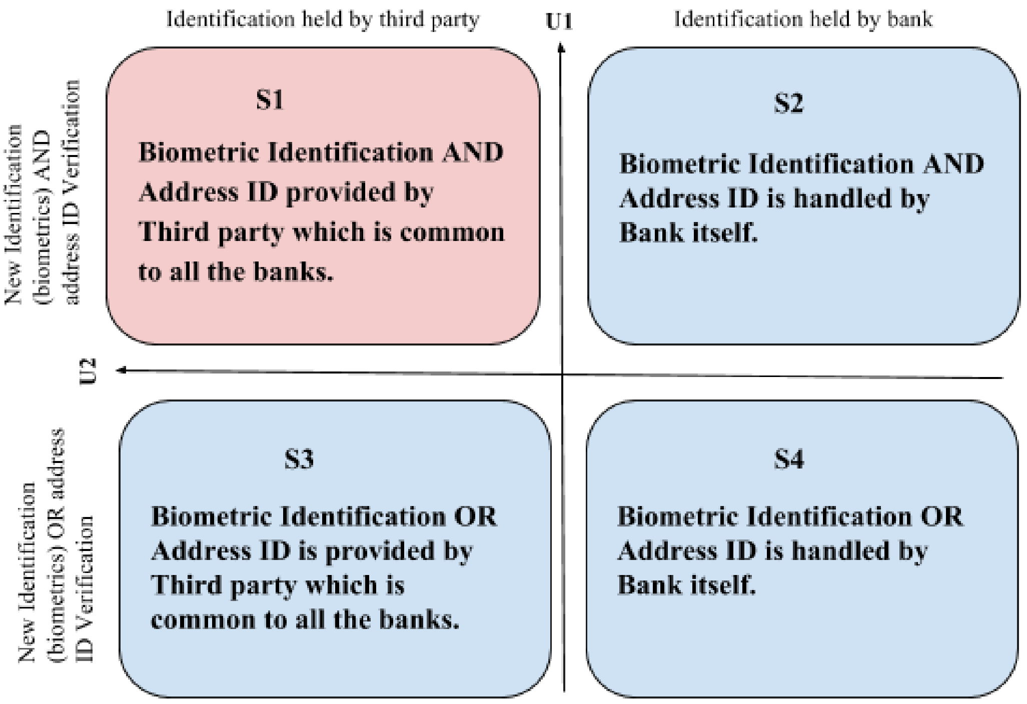

Identification held by third party
U1
Identification held by bank
New Identification (biometrics) AND address ID Verification
S1
Biometric Identification AND Address ID provided by Third party which is common to all the banks.
S2
Biometric Identification AND Address ID is handled by Bank itself.
U2
New Identification (biometrics) OR address ID Verification
S3
Biometric Identification OR Address ID is provided by Third party which is common to all the banks.
S4
Biometric Identification OR Address ID is handled by Bank itself.

Figure 3 : Initial Scenarios

Scenario 1 which is represented as S1 explains about the scenario when there is the security check upto 2 levels which includes biometric identification and the address ID verification. This is carried out by third party company which can be government as well. This requires a common database for the banks.

Scenario 2 which is represented as S2 explains about the scenario when there is the security check upto 2 levels which includes biometric identification and the address ID verification. This is carried out by bank itself without being dependent on any other third party companies. There will not be any common database which is shared between the banks and each bank will have its own database of the personal information of the customer.

Scenario 3 which is represented as S3 explains about the scenario when the security check upto 2 levels is not required for the initial authentication service while opening a bank account. It can include either biometric identification or the address ID verification. This is carried out by third party company which can be government as well. This requires a common database for the banks.

Scenario 4 which is represented as S4 explains about the scenario when the security check upto 2 levels is not required for the initial authentication service while opening a new bank account. It can include either biometric identification or the address ID verification. This is carried out by bank itself without being dependent on any other third party companies. There will not be any common database which is shared between the banks and each bank will have its own database of the personal information of the customer.

Among the listed scenarios, Scenario 1 is more feasible for this case study as it has two levels of strong authentication which is high secured i.e having both the biometric identification and the address ID verification will give us high level of security to avoid any problems in future. This is carried out by a third party which can be government. The main role of this third party is to have strong authentication service and also a common database of the customers whose details are up to the date. This database can be used by the banks at any point of time whether it is to open a bank account at start or to send any document through mail in future.

4.2. VNC (Value Network Configuration)

The first step of VNC method was to identify the actors. The actor are involved directly in the VNC, you need to have a contract between them. It is only the most important one. For this in use our previous work in the scenario analysis. We find three actors based on our scenarios: Bank (S-Pankki), the future bank customer (the end-user, maybe not good because future) and identification third party (for example Government).

The second step was to going deeper in the case by defining the business roles. The third step was the last level how we can provide those business role. It is actual piece of software (for example Mobile bank application), piece of hardware (for instance mobile phone with camera).

The interest to do a VNC is to see clearly in one diagram the structure of the service. Ii is really powerful. We can see in this single diagram the three layers: actors, business roles, and technical component. It allow to see how the service will work technically and also how we will earn money. We can see the interface (technical and business) between the actor. We see how the technical component we will split between the actors.

We choose to focus on one main VNC, and three alternative one which they are in correlation with our four scenarios. We think that these VNC could happen in the scope we fixed previously. We try to clarify this scenario by using VNC and with a short description of this one.

The first VNC is about biometric Identification and Address ID provided by third party (exemple gouvernement) common to all the banks. We choose this VNC because we think that it will be in this configuration than the service is more likely to involve.

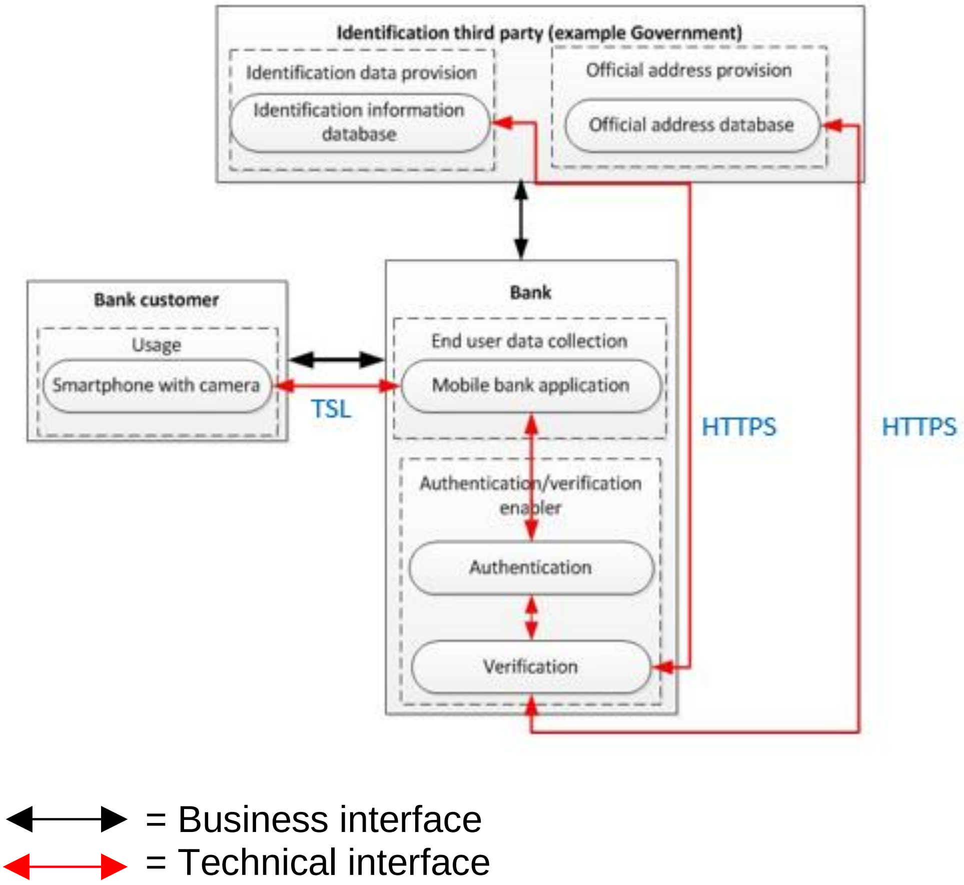

Identification third party (example Government)
Identification data provision
Identification information database
Official address provision
Official address database
Bank customer
Usage
Smartphone with camera
TSL
Bank
End user data collection
Mobile bank application
Authentication/verification enabler
Authentication
Verification
HTTPS
HTTPS
= Business interface
= Technical interface

Figure 4: Third party driven VNC.

In the VNC, the process is still pretty similar to the one which is actually use (check with the population register). It will be easier to put the process working efficiency. Point of view of technical interface, we use a smartphone to take a picture of the ID, we are losing some security if we just need to stole an ID. To compensate this issue we use another database with a biometric information, we can use the fingerprint, face recognition, voice recognition). The bank customer will need to download an application via (playstore or apple store). This application will be the same than S-pankki have already. The application will have the right to access to your camera, your microphone for the identification. We use the TSL (Transport Layer Security) protocol to communicate between the application on the phone and the bank's server. The bank will gathering the information and send to the third party by a HTTPS (Hypertext Transfer Protocol Secure) protocol. The third party have a database. If we

have a valid identity, the bank will allow the customer to open a bank credential.
One of the problem, is the database, it need to exist. The one for the address already exist. We still need to make database for fingerprint or something else (by biometric passport for example).

Point of view of business interface, the investment will be in the development of the mobile application and the implementation in the bank's application. They will need to pay the maintenance of the application and a service client. For the service providing by the third party : the bank will need to pay in a forfait, or it could be free if it is provided by the gouvernement. For the customer, it can have some advantage to choose this new identification compare to go to the bank office.

S-pankki have already a lot of data in customer (they own also S-market). Moreover, if S-pankki it is faster than this other, they would not want to wait and decide to provide the service and own the database. In this case we will have this VNC: Biometric Identification and Address Id is handled by bank itself.

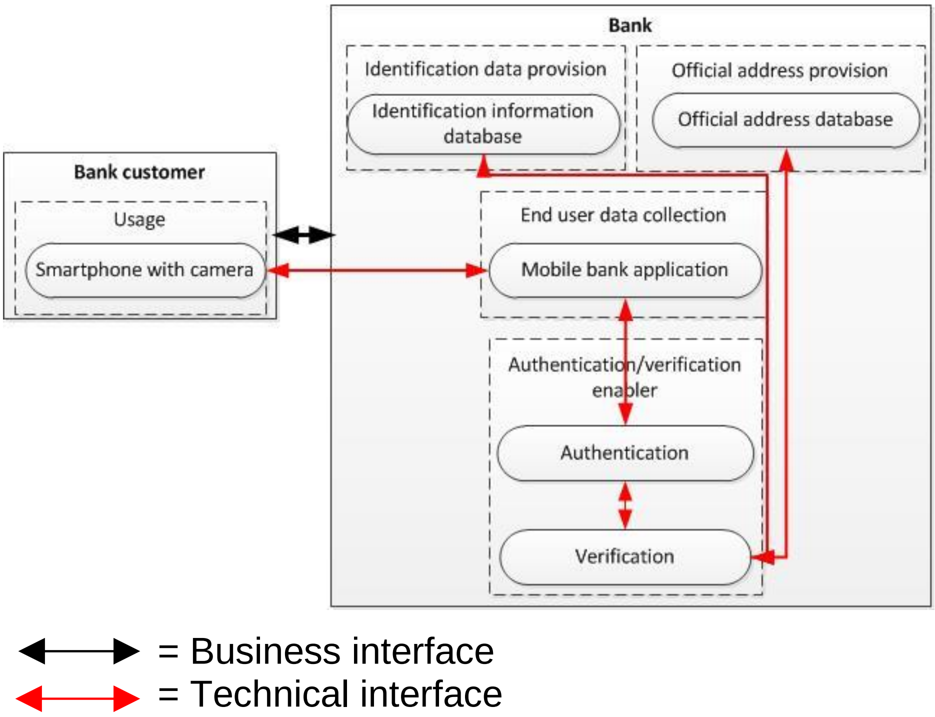


Figure 5: Bank driven VNC.

The configuration add new problem for the bank. It needs to take care the problem of the database, need more investment and harder to provide the service quickly than the first VNC.

With the two next VNC, we decide than 1 level of security is enough. It is some alternative of VNC. It will work the same than previous but with only one. The first one with the Biometric Identification OR Address Id provided by Third Party/Govt common to all the banks.

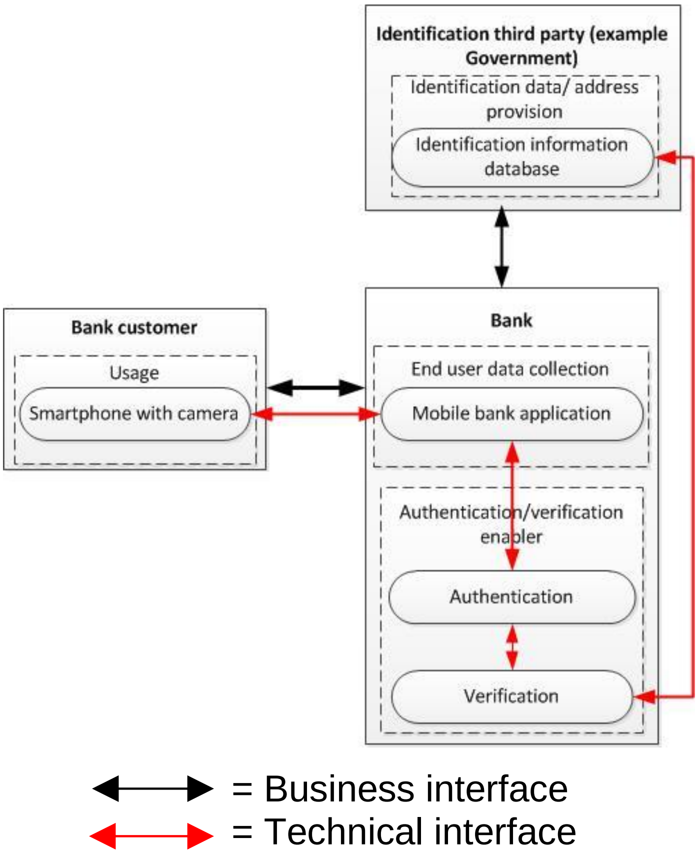


Figure 6: Third party driven VNC version 2 (only one identification information provided).

In the final VNC the bank will driven Biometric Identification OR Address ID is handled by Bank itself.

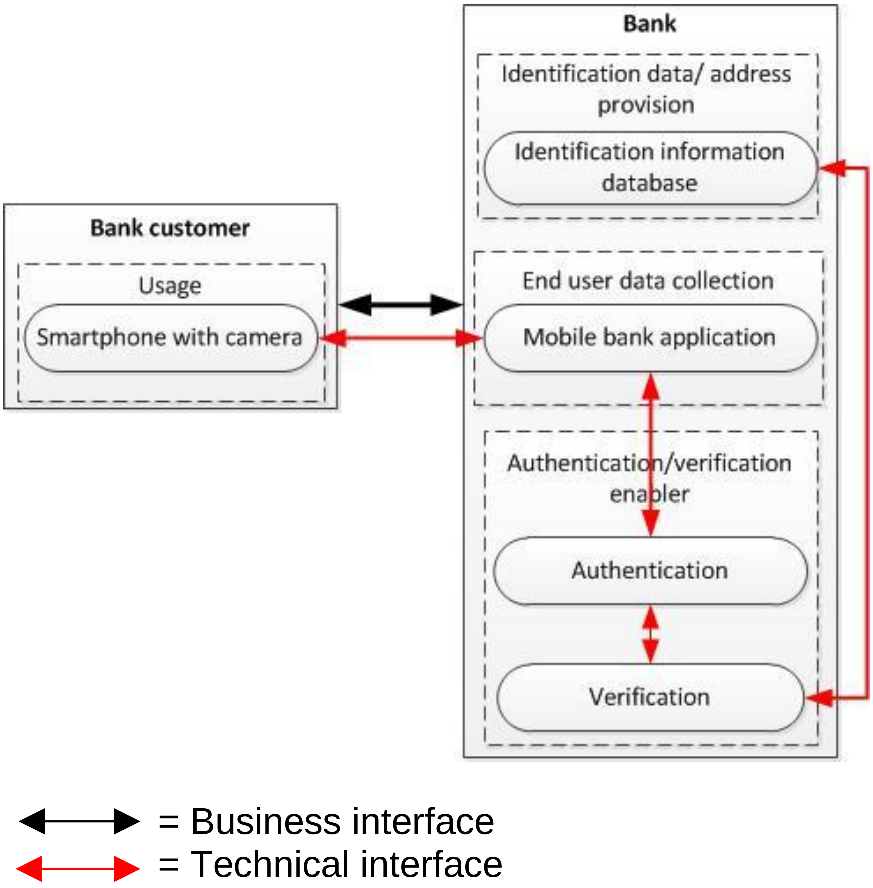


Figure 7: Bank driven VNC version 2 (only one identification information provided).

4.3. STOF

As mentioned in chapter 2, The STOF model has four domains: Service domain, Technology domain, Organizational domain and Finance domain and these can be analyzed with STOF method. The method consist of four steps: Quick scan, evaluation of critical success factors, specifying critical design issues and making a robustness check. (Bouwman et al. 2008)

To analyze initial authentication business case, we started with Quick Scan step and finding out answers to the basic business questions. In service domain, the value for the customer is that getting the bank credentials via identification in mobile phone app is faster way to get the bank credentials than visiting the bank. In technology domain, the main components needed to create a mobile phone application that communicates with other service provider are mobile phone application, camera for identification, API's between application and third party database. In organizational domain, the organizational structure for the service is quite simple: The business is run by the bank and identification service provider that might be third party or government. Quick scan results for finance domain showed that key for the financial balance and revenue creation is the business model between bank and third party/ government that need to be well defined.

The second step of the STOF method is defining critical success factors. The success factors for the initial authentication case can be grouped in user experience and user value, technical issues and security issues. In user experience point of view, the application should be user friendly and easy to use and erase the requirement to visit the bank. Also in problem situations support should be available online or via same application. All target groups should be taken into account. The application should also have good performance, since it is searching data from third party database. There shouldn't be any long delays in data collection via API. Technically the API between the bank and third party should be created with secure connection. Data that goes through the API is personal identification data and if it leaks it is very risky. Also identification technology should be very secure and the identification valid. Business model should be beneficial for both the bank and third party /government. The third step of STOF method is specifying critical design issues. Critical Design Issues will be specified in the following sub-chapters.

4.3.1. Critical Design Issues for Service domain

The main goal in service doman was to find the service value for the customer. The service should be targeted to customers without previous bank credential. These customers can be any age, immigrants or Finnish citizens. The value why they would use the mobile application initial authentication to get bank credentials is that it is faster way to get the credentials and there is no visit to the bank office needed. In bank perspective, less bank officers are needed since there are less customer visits to the bank. Bank credentials would also be delivered in more efficient way. Also, when using mobile phones, the bank credentials might not be sent by mail: banks are already planning to have OTP lists in mobile phones (Yle.fi, 2017). Mobile application initial authentication service would create value for the customers, but there are security aspects to tackle: When there is secure enough identification service available to fulfill the customer needs? Trust for the service is strongly related to its security. How to build trust for the new service when there are not yet real customer experiences and identification data is very sensitive?

One aspect in service domain is branding. S-Pankki already has a strong brand image, but branding would be needed to the new service. Media and communication agencies could help S-Pankki to create a good and interesting image to the new service. Also advertising would be needed to create customer awareness. In customer retention point of view, actual banking services has more important role: initial authentication and identification service is needed only once to create the new credentials. The results from the Service domain are gathered to the table below.

CDI	Description	Balancing requirements
Targeting	End user without any previous bank credentials	Old or young customers, Finnish people or immigrants/ exchange students
Creating value	Quicker way to get bank credentials, No queuing in the bank, Less bank officers needed, Efficiency for bank credential delivery,	End user needs for faster service vs technology and security aspects
Branding	S-Pankki has already strong bank image in Finland, Branding for the new service is needed	S-Pankki brand vs. identification service brand, New service brand vs.old brand
Trust	Trust for the identification and authentication	Security vs ease of use
Customer retention	Service is needed only one -> brandimage more important than retention	

Table 1: Service domain CDI's and balancing requirements.

4.3.2. Critical Design Issues for Technology domain

As mentioned in service domain, security topics are strongly related to the service value in S-Pankki case. In technology domain's security aspects, integrated connection between mobile application and identification database must be super secure. Authentication and authorization information is sent only to identification database and there should be no data leakage. The application and identification and address information databases work correctly and with secure connection together. Level of the quality ofthe service should be good: application software is performing correctly and customer flow of the usage is logical. Customer should also be informed how the identification service works and what are the security aspects. Application should be available for the most common mobile phone platforms that include good enough camera. If the customer mobile phone doesn't fill the requirements, he or she i redirected to other service. The DCI's for technology domain are gathered to the following table.

CDI	Description	Balancing requirements
Security	Data integrity in the database, Authentication and authorization information is sent only to identification database, Identification service technology is secure, Apps/ softwares work correctly together	Privacy vs security, Efficiency vs abuse
Quality of Service	Bank software performance, The customer is informed about identification service usage	Quality vs costs
System integration	Integration between bank software and identification database provider	Flexibility vs costs
Accessibility	Bank mobile application support for different mobile phone platforms/ cameras	Security vs accessibility
Management of user profiles	New customer information is sent to bank customer database	User involvement vs automatic information flow

Table 2: Technology domain CDI's and balancing requirements.

4.3.3. Critical Design Issues for Organizational domain

Organizational domain CDI's concentrate in network structure of the service. In the chosen business model, the service is governed by the bank. The network is very simple and consist of the bank and the identification information provider, that could be government or third party. When the identification and address databases are provided by separate service provider, the partner needs to be chosen carefully. Also authentication and authorization protocols could be provided by someone else than the bank. Then partner selection needs to be thought also for these services. Network openes point of view, in the chosen case the network is closed and there are only the bank and identification service provider. The case could also be that for example all the banks in Finland use the same third party identification information and address provider. Network would be even wider if the identification service providers provides their service to other customers than banks only. The results from the organizational domain are gathered to the table below.

CDI	Description	Balancing requirements
Partner selection	Authentication and authorization in bank software and identification database by partner	One partner vs several partners (for also authorization and authentication)
Network openness	Partnership with one certified identification database provider	Control and security vs wider identification possibilities
Network governance	Governance by bank	Centralized vs distributed governance
Network complexity	Simple network (bank and identification database)	

Table 3: Organizational domain CDI's and balancing requirements.

4.3.4. Critical Design Issues for Finance domain

For finance domain, the DCI's are related to pricing and investments. For pricing the service, there are two way to charge the customer: price for opening the account and price for maintenance of the bank account. There could also be price for credential creation via the mobile application - or other way around, extra price when the bank credentials are created when visiting the bank office. The mobile application service could also be for example free for non-employees and student and charged for employees and non-students. To get more people to get bank credentials via mobile application, the cheaper the price for that the better. Since there could be some price that people were willing to pay for the faster way to get the credentials than visiting the bank. The whole revenue flow plays the key role here. There will be integration costs and costs for authentication and authorization technology creation, so that money could be compensated with some revenue. When more people are creating the credentials via bank mobile application, banks might need less bank officers what is savings for personal costs. There could also be some investors, that would be interested to invest to the service development. The combined results from finance domain are gathered to the following table.

CDI	Description	Balancing requirements
Pricing	Opening bank account charge, Maintenance of the bank account	Free for students vs charge for non-students, Free for non-employees vs charge for employees
Investments	Integration costs, Investment for authentication and authorization services	End user vs bank vs investors, Capital investment vs risk assessment

4: Finance domain CDI’s and balancing requirements.

5. Conclusions

In this report we presented Initial authentication service case for Aalto University course Value Network Design for Internet Services. The case was analyzed with scenario analysis method, value network configuration method and STOF method. The most important findings were:

- The new service for providing the bank credentials is that the users would use anks mobile application, identify themselves with biometrical identification and address and get the bank credentials
- To provide two level initial authentication, banks can cooperate with third party who provide identification and official address information. Another solution is that bank owns the databases.
- Security of the service is in very important role since there is personal information moving the application and the databases.

In the validity point of view, the results make sense. The biggest issue for starting the service is that there isn’t yet found possible service provider to provide identification database service. The actor could be government or third party. S-Pankki could also create their own database, but we wouldn’t necessarily recommend this solution since providing banking services is the main business of the banks.

For future research, secure enough identification services could be investigated. Is there secure enough identification information available to minimize the misuse of the service? What company would cooperate with banks to provide the identification database? Will bank credentials still be used to access public services or could there be other options?

References

[1] Bouwman, H., De Vos, H. & Haaker, T. eds., 2008. *Mobile service innovation and business models*. Berlin: Springer. Rahoitusvakausvirasto., 2017. *Pankkiluettelo*. [Internet] Available at: http://rvv.fi/pankkiluettelo [Accessed 20 April 2017].

[2] S-Pankki., 2017. *How to get bank credentials?* [Internet] Available at: https://www.s-pankki.fi/fi/arjen-raha-asiat/verkkopankki/nain-saat-tunnukset/ [Accessed 20 April 2017].

[3] Suomi.fi., 2017. *Information about e-services and forms in Suomi.fi* [internet] Available at:https://www.suomi.fi/suomifi/english/eservices/information_about_eservices_and_forms_in_suomifi/index.html [Accessed 20 April 2017].

[4] Suomi.fi., 2017. Logging in with bank identifiers. [internet] Available at: https://www.suomi.fi/suomifi/english/eservices/electronic_identification_and_digital_signature/logging_in_with_bank_identifiers/index.html [Accessed 20 April 2017].

[5] Workinestonia.com., 2017. [internet] Available at: https://www.workinestonia.com/coming-to-estonia/personal-id-code/#articleblock-EstonianidentificationcodeviaE-Recidency [Accessed 20 April 2017].

[6] Nordea.fi., 2017. [internet] Available at: https://www.nordea.fi/en/personal-customers/everyday-finances/internet-mobile-and-phone-services/access-codes.html [Accessed 20 April 2017].

[7] OP.fi., 2017. [internet] Available at: https://www.op.fi/op/op-ryhma/opastus/verkkopalvelun-kaytto/verkkopalvelutunnukset?id=87120&srcpl=8 [Accessed 20 April 2017].

[8] Danskebank.fi., 2017. [internet] Available at: https://www.danskebank.fi/en-fi/Personal/online-services/bank-ids/Pages/bank-ids.aspx [Accessed 20 April 2017].

[9] Taloussanomat.fi., 2017. *Suomen suurpankit näyttävät vahvemmilta kuin ovat.* [internet] Available at: http://www.is.fi/taloussanomat/porssiuutiset/art-2000001815087.html [Accessed 20 April 2017].

[10] BankID.com., 2017. [internet] Available at: https://www.bankid.com/en/om-BankID.no. (2017). bankid/detta-ar-bankid and https://www.bankid.no/en/about-us/ [Accessed 20 April 2017].

[11]Yle.fi., 2017. *Verkkopankkien pahviset tunnuslukulistat voivat olla pian historiaa* [internet] Available at: http://yle.fi/uutiset/3-9240095 [Accessed 20 April 2017].

[12] Casey, T., Smura, T. & Sorri, A., 2010. Value Network Configurations in Wireless Local Area Access. In: *Proceedings of the 9th Conference of Telecommunication, Media and Internet Techno-Economics (CTTE)*. Ghent, Belgium.

[13] Heikkinen M., Casey T,. Hencht F. (2010). *Value analysis of centralized and distributed communications and video streaming.* VOL. 12 NO. 5 2010, pp. 42-58, Q Emerald Group Publishing Limited, doi: 10.1108/14636691011071158

[14] Schoemaker, P.J.H., 1995. Scenario planning: a tool for strategic thinking. *Sloan Management Review*, 36, pp. 25–40.

[15] Wikipedia.org (2017). S-Pankki.[internet] Available at: https://en.wikipedia.org/wiki/S-Bank [Accessed 24 April 2017].

[16] The Financial brand (2017). *Mobile banking account opening options.* [internet] Available at: https://thefinancialbrand.com/38297/mobile-banking-account-opening-options/ [Accessed 24 April 2017].
[17] Wikipedia.org (2017). *Immigration to Finland* [internet] Available at: https://en.wikipedia.org/wiki/Immigration_to_Finland [Accessed 24 April 2017].
[18] Darrell M. West and Joshua Bleiberg(2014) [internet] Available at: https://www.brookings.edu/blog/techtank/2014/09/15/the-explosive-growth-of-the-mobile-economy-will-change-the-world/ [Accessed 24 April 2017].

Feedback for the course

The concept of the course was good and lectures and presentation sessions worked well together. The structure of the course was nice, since there was deadlines every two weeks for different methods and well time to create the final report. The opponent report helped us get more clarity on our case. The workload was spread during the course and was suitable for 5 credits. Idea to have different case and contact person for different cases made the case and working with it more interesting.

Methods in the course worked quite well to S-Pankki case. The more difficult methods to use in the S-Pankki case were scenario and VNC, but after working with those it was easier to use STOF method. For scenario analysis, it was easy to choose service providers to horizontal scale but more difficult to define the vertical scale. For VNC defining technical components needed more time to work and think than defining the actors.

It was nice to get quite much feedback in the lectures. It helped a lot to learn how to use different methods and how to improve the presentation. Our group got quite much feedback to scenario analysis and it would have been good to have more feedback to STOF. Still, it is understable since scenario analysis was basis for VNC and STOF and it was important that it was done correctly.