TALLINN UNIVERSITY OF TECHNOLOGY

Faculty of Information Technology

Department of Computer Science

TUT Centre for Digital Forensics and Cyber Security

ITC70lt

Kadri Talvoja 144015 IVCM

USABLE SECURITY OF TWO FACTOR AUTHENTICATION METHODS

Master thesis

Jaan Priisalu

Master’s degree

Tallinn 2016

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Kadri Talvoja

04.01.2016

Abstract

The aim of the thesis is to evaluate usable security of two factor authentication methods used in e-services in Estonia. The present paper uses the Estonian state portal, eesti.ee, as a case study.

This paper had **four hypothesis**. The first two hypothesis (H1 and H2), that authentication methods differ from each other in their usability and security aspects, were proved. Hypothesis (H3) that authentication methods that score high in usability and score low in security, was disproved contrary to previous studies done regarding the usable security of authentication methods. The fourth hypothesis (H4), that users evaluate usable security of authentication methods rationally, was also proved.

Usability was evaluated by conducting a survey, usability tests and analyzing server logs. During the usability test, participants' brainwaves were also measured in order to capture their satisfaction the best possible way. The security of each authentication method was measured with attack trees. These methods proved to be a good way to evaluate usable security. However, having a greater number of participants in the survey and usability tests would offer more valuable insights.

This thesis is written in English and is 57 pages long, including 5 chapters, 8 figures and 13 tables.

Annotatsioon

Usable Security of Two Factor Authentication Methods

Lõputöö eesmärgiks oli hinnata kahefaktoriliste autentimismeetodite turvalisuse kasutuslihtsust. Täpsemalt uuris käesolev töö seda Eesti riigiportaali, eesti.ee, näitel. Töö keskendus nelja autentimismeetodi - ID kaardi, mobiili ID, panga PIN kalkulaatori ning panga paroolikaardi - hindamisele. Neid autentimismeetodeid rakendatakse laialt ka teistes Eesti e-teenustes ning seetõttu annab töö hea ülevaate autentimismeetodite turvalisuse kasutuslihtsusest ka teistele e-teenuste haldajatele ning loojatele.

Lõputöö käigus tõstatati **neli hüpoteesi**. Esimene hüpotees, et autentimismeetodid erinevad üksteisest kasutuslihtsuse poolest, kinnitati. Samuti kinnitati teine hüpotees, et autentimismeetodid erinevad üksteisest turvalisuse poolest. Kolmas hüpotees, et autentimismeetodid, mille kasutuslihtsus on suur, on madala turvalisusega, lükati ümber. Neljanda hüpotees, et kasutajad hindavad autentimismeetodite turvalisuse kasutuslihtsust ratsionaalselt, kinnitati.

Selleks, et autentimismeetodite turvalisuse kasutuslihtsust hinnata, oli vaja turvalisust ning kasutuslihtsust hinnata eraldi. Turvalisust hinnati ründepuude abil, omistades ründevektoritele kolm väärtust – ründe õnnestumise tõenäosus, ründe õnnestumise tehniline ning äriline mõju ja riskitase. Kasutuslihtsuse mõõtmiseks viidi läbi 393 vastajaga küsimustik, 20 osalejaga kasutajatest ning ühtlasi uuriti ka serveri logisid. Kasutajatesti raames mõõdeti kasutajate ajulaineid EEG masinaga, et näha, mis tundeid autentimine neis tegelikult tekitas.

Uurimistöö käigus kasutatavad meetodid olid sobivad hindamaks turvalisuse kasutuslihtsust ning töö andis hea ülevaate turvalisusest ning kasutuslihtsusest. Selleks, et teha veelgi täpsemaid otsuseid selle kohta, et kuidas autentimismeetodeid turvalisemaks ning kasutuslihtsamaks teha, tuleks uurimistööd laiendada. Näiteks turvalisuse osas tuleks kohandada ründe tõenäosuse väärtusi ning neid täpsemalt analüüsida erinevates kontekstides. Kasutuslihtsuse osas oleks hea laiendada vastajate arvu.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 57 leheküljel, 5 peatükki, 8 joonist, 13 tabelit.

Table of abbreviations and terms

CA	Certification Authority
EEG	Electroencephalography
et al.	*et alia*; and others
H	hypothesis
I	Impact in attack trees
ISO	International Organization for Standardization
MITM	Man in the middle attack
OTP	One Time Password
P	Probability in attack trees
PIN	Personal Identification Number
PKI	Public Key Infrastructure
R	Risk in attack trees
RSA	Rivest Shamir Adlemann algorithms
SSL	Secure Sockets Layer

Table of contents

List of Figures

List of Tables

1. Introduction

For the past 15 years an increasing number of our daily activities have continued to move online, from personal shopping to declaring taxes. The various online environments hold sensitive and financial information which needs to be protected from malicious users. At the same time, that information should be easily accessible for legitimate users, so they can conduct their daily tasks more conveniently. To ensure that users really are who they claim to be, owners of online environments require their users to authenticate themselves.

Authentication is seldom the primary goal for users. Thus users generally regard authentication as a nuisance. When a secondary goal, such as authentication, takes a long time to accomplish and is inconvenient, users generally try to find ways to avoid it. Strong authentication methods, such as two factor authentication, are more secure than many other authentication methods. However, these can be time-consuming and can drain the productivity of the user more than weaker authentication methods, such as knowledge based passwords [25], [53].

Organizations which request that users authenticate for security purposes, might face harsh reality when users stop using their services altogether, if the authentication process is made too inconvenient. It is important to understand the effects of different authentication systems, so organizations can find the best possible authentication method which would not only be easy for users to use, but would be secure for the organizations so their assets will remain protected.

The present paper focuses on usable security of two factor (2F) authentication methods. 2F authentication is an authentication process which uses two recognized factors from three – something you know, something you have (the token) and something you are - to authenticate the user. Since 2F authentication uses more than one piece of information for authentication, it is considered to make authentication more secure.

2F authentication methods are widely deployed in Estonian e-services, thanks to a well-functioning and extensively used public key infrastructure. However, there has been no notable research done regarding the usable security of 2F authentication methods in Estonia. Thus, little is known regarding how users feel about using them.

The aim of the present research is to find out which two factor authentication method used in Estonia works best, in terms of usability and security. The present paper has chosen the Estonian state portal, eesti.ee, as a case study. The authentication process used by the state portal is very similar to authentication processes deployed by many other e-services in Estonia. Thanks to this, the results of the research in this paper are applicable when considering the design of authentication system in other e-services.

The present paper measures only one part of the authentication process – authentication function. The present paper does not include rollout of the authenticator and transaction processing. It is also assumed that organizations responsible for issuing authentication tokens, and managing authentication process, do not have malicious intentions.

This research paper is divided into five main parts. The first part of this paper takes a deeper look into existing research regarding usable security of authentication methods. The second part explains the methodology of the current research paper and states four hypothesis. The third part presents the findings. The final part of this paper is the conclusion.

2. Related research

According to Yee et al. [54], a system which is more secure is more controllable and reliable, which makes it more usable. The more usable a system is, the easier it is to use as intended, which also increases security. Kainda and Yao have conducted studies which show that when choosing an authentication method to deploy, the usability and security aspects both need to be taken into account in order for the system to function well [28], [53]. Though usability and security are interdependent, in the field of usable security, usability and security dimensions are usually measured separately.

Authentication methods diverge on the levels of security and usability they offer, and their usability and security are often taken for granted, with little empirical research to back them up [4], [9]. There is also no standard approach for evaluating and comparing authentication methods. To compare them, some studies use heuristic evaluation, during which user interface experts evaluate the process. Other comparison methods have used usability tests with real users. Some studies are conducted in test environments, while others utilize live environments [12], [24], [50]. Attributes which are being compared vary greatly from study to study. Regardless of the research methods used, studies on authentication methods have repeatedly pointed out the conflict between usability and security. De Cristofaro et al. have even come to the conclusion that there seems to be no authentication method better in both usability and security, than all other methods.

A lot of research on authentication methods has been done in the field of memorability, or cognition. Those studies have mostly concentrated on knowledge-based authentication and they have concluded that people tend to forget passwords, choose passwords that are weak, disclose their passwords to others and write them down. All of this decreases security [41], [50]. Researchers have not observed that users remember graphical passwords better than other types of passwords, even though graphical authentication is often considered easier to use in terms of memorability [5], [9], [28], [53].

Recently, more research has been conducted in 2F authentication, due to its increasing popularity. For example, Weir et al. [50] conducted a study which investigated customers' perception on usability, convenience and security. The research concentrated on comparing different authentication methods that use OTPs. All the OTP authentication

methods which were studied, differed in their usability and security. The research established that users value usability and convenience over security. The study demonstrated that the authentication method which was considered most usable, push-button token, was perceived the lowest in security. Cristofaro et al. [12] conducted a usability study in which they compared three 2F technologies – codes generated by security tokens, OTPs received via email or SMS and dedicated smartphone apps. They discovered that usability and security depended on people's characteristics and on the context, more than on actual technologies.

Usability

Even though usability is largely contextual, there are certain known attributes which can determine the usability of an application. Some of these attributes vary slightly from research to research, but the ones which are consistently mentioned in every usability research paper are **effectiveness, efficiency** and **satisfaction.** The International Organization for Standardization (ISO) also defines usability by these three attributes [28], [52].

While usability attributes of researchers like Yao and Feng [53] and Cristofaro et al. [12] match ISO's definition almost entirely, many researchers have expanded the list of usability attributes significantly. For example, Jeffries et al. [24] has added - learnability and memorability to the list. Kainda et al. [28] has added accuracy, memorability and knowledge/skill. Braz et al. [4] have gone even further, and listed 9 usability attributes in their usability model. Renaud [38] has not listed attributes exactly, but has listed aspects which need to be considered with respect to usability of authentication methods. For example, she has added enrollment time and replacement time of authenticators to her list.

The present research paper focuses on the three main usability attributes - effectiveness, efficiency and satisfaction - and measures those attributes in order to evaluate the usability of different 2F authentication methods which are deployed by the state portal. Additional attributes are not included because, though they are mentioned by different scholars, they're regarded as sub-attributes of the three main attributes. Thus, by measuring the three main attributes, it is already possible to cover the impact of sub-attributes.

Before we start measuring effectiveness, efficiency and satisfaction, it is important to understand what each of those attributes really are and how they can be measured.

- **Effectiveness** – A system is only useful for users if the users are able to complete the goals, which they were aiming to achieve, accurately [28], [50]. Yao and Feng [53] measured it with a rate of successful logins to the system, Weir et al. [50] and Kainda et al. [28] measured it in terms of task completion.
- **Efficiency** – Users' tasks need to be achieved within an acceptable amount of time and effort. Obviously what is considered an acceptable time will vary from system to system, but it can still be measured in a precise way. Yao and Feng [53] measured it as the time a user spends on creating user name and password during the first visit. Kainda et al. [28] measured it with the time that it took to complete a goal; or with the number of clicks/buttons pressed to achieve required goal.
- **Satisfaction** – Systems must be acceptable and comfortable for users. However, this is very subjective because what is acceptable for one user, might not be for another [4], [28], [52]. There is no single way to measure satisfaction, and not much research has been done on measuring it. That is why different scholars have been using different methods of measurement. For example, Yao and Feng [53] used NASA-TLX tool for measuring satisfaction. It is a multi-dimensional rating procedure which provides an overall workload score based on a weighted average of ratings on six sub-scales (mental demands, physical demands, temporal demands, own performance, effort and frustration). Weir et al. [50] and Cristofaro et al. [12] used attitude questionnaires after each experience that employed a Likert scale. Kainda et al. [28] measured satisfaction through interviews and rating scores.

Security

Security is all about protecting systems and information from malicious attackers. Even though security concentrates mostly on malicious attackers, it is important that non-malicious users are not ignored as they are also capable of compromising systems [28].

There is no single way that the security of an authentication system can be measured, so different scholars have approached it in different ways. Some researchers have asked users to rate their feelings about security aspects of authentication method, others have used more empirically measureable criteria. Yao and Feng [53] evaluated security by

measuring three aspects – difficulty of guessing the password, difficulty of brute force attack and the difficulty of describing and sharing the key with other users. Kainda et al. [28] listed five security factors that need to be measured when talking about security – attention, motivation, memorability, social context and conditioning. A problem with the Kainda et al. security factors is that they largely overlap with usability factors, and it is difficult to separate usability and security factors from each other when using his classification of usability and security. Renaud [39] quantified the quality deficiency of predictability of the password, abundance of the possible authenticators and disclosure as the key aspects. Even though Renaud gave concrete numerical values in her research, those values were initially subjectively determined.

Unfortunately, none of the approaches used in the research of usable security of authentication methods offers a systematic and easily measurable solution for evaluating security. However, there are other methods for assessing the security of applications and systems.

One way to discover the security of an application is to use attack modelling, and one of most widely known techniques of such modelling is called **attack trees** [47]. Attack trees are believed to have been in usage since the late 1980s by the intelligence community, and they have been recently popularized by Bruce Schneier [22]. Attack trees can be created graphically or textually, the latter being used for more complex systems [15]. In an attack tree, different attacks are presented in a tree structure, with the root node as the ultimate goal of an attacker. The attacker's different actions to achieve that goal are represented as leaf nodes. Intermediate nodes are sub-goals which need to be satisfied for achieving the ultimate goal [13], [15], [42].

In an attack tree, there are AND and OR nodes. AND nodes represent different steps towards achieving the goal. Additionally, an AND node requires all of its children nodes to be satisfied in order to achieve the ultimate goal. OR nodes are alternatives, so they only require a single child to be satisfied to achieve the ultimate goal [15], [42].

Different value attributes can be assigned to nodes of attack tree. Weiss, Salter, Edge et al., Buldas et al., Jürgenson et al. and others have used attributes such as probability, cost, penalty of a success and/or impact. But other attributes can be assigned as well. Values of attributes can vary as much as attributes themselves, since there is no universal system that has to be used in attack trees. It is possible to use real numbers or use nominal scale

values, such as low, medium, and high. It's also possible to use Boolean values, or some other type of value system, depending which one is the most adequate for a specific instance [3], [43]. When values of attributes are combined, it is possible to understand what vulnerabilities the application or system has, and how secure it is [15], [42].

An attack tree presents a perspective of the whole system. It identifies known attacks and provides details on how attacks against the application or system can be carried out. This, in turn, can enable service providers to make security decisions, because it surfaces their vulnerabilities and can help mitigate attacks. Attack trees offer a very methodological approach to determine security levels, and this is the reason that the present research uses attack trees to measure security of different 2F authentication methods.

3. Methodology

3.1. Research environment

This paper researches usable security of authentication methods of **Estonian state portal eesti.ee.** The portal is an environment through which Estonian residents access the state's e-services, contacts and information [46]. In 2014, this portal had more than 4.5 million visits by 401 316 users (30.5% of Estonian population) [46]. Users can take the role of a citizen, entrepreneur or an official. They also choose the service they need for their particular role. The portal can be entered by authenticating yourself via several available 2F authentication methods.

Based on the Estonian Information System Authority data from six months of 2015 (May through October), the majority of state portal users authenticate themselves using their ID card – 61.2% of all authentications. Authentication via the biggest banks, Swedbank (18%) and SEB (8.4%), is also popular. 9.6% of users authenticate themselves via mobile ID. Figure 1 shows the usage of different authentication methods in login to state portal.

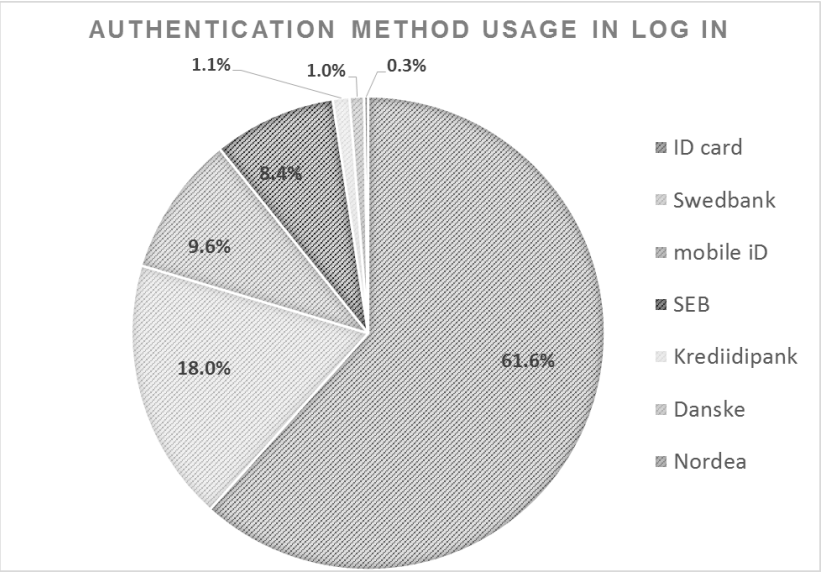

Figure 1. Usage of authentication methods in state portal.

3.2. Design of authentication methods

Users can enter the portal by choosing to authenticate themselves in one of the three types of authentication methods available. Those methods are:

- **ID card:** Estonian ID cards are issued by Citizenship and Migration Board for all citizens and foreigners, who have residence permit. More than 90% of inhabitants in Estonia have an ID card [16]. ID card can be used for electronic identification and it is possible to give digital signatures with it. The card has an electronic chip which contains a personal data file, and each user is paired with private and public key for which a trusted authority issues a matching digital certificate. Private Key on the card can be unlocked with PIN1 [18], [46].

Authentication with the ID card to a service (state portal) works as follows (Figure 2):

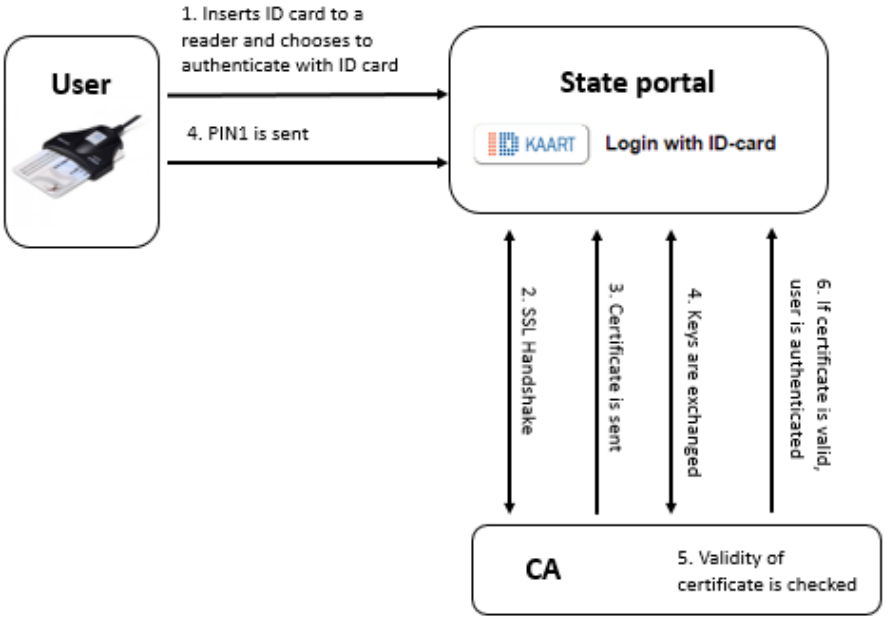

Figure 2. Authentication process with ID card.

1. The user has to insert the ID card into a reader and choose to authenticate with ID card in interface;
2. A certificate authority (CA) server and the client are establishing a session, SSL handshake is done. During this process, the server and client agree on an

authentication protocol, transportation key and in other technical parameters needed for the session;

3. The server sends the certificate to a client to give information about itself;
4. Transport keys are exchanged;
5. The server checks if certificate is valid;
6. If the certificate is valid, the user is authenticated and the service provider reloads a logged in screen.

- **Mobile ID:** Mobile ID is issued by the mobile phone operator for 3 years. Private keys are stored on the mobile SIM card along with a small application for authenticating and signing. Mobile ID is activated after registration at the Police and Border Guard Board [33].

Mobile ID authentication works as follows (Figure 3):

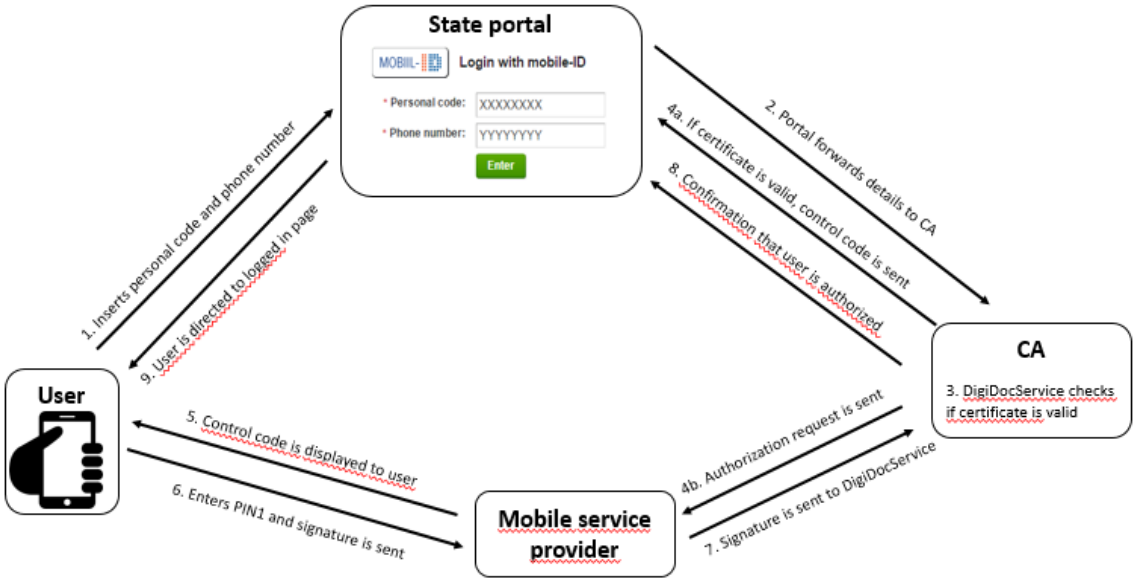

Figure 3. Authentication process with mobile ID.

1. The user has to enter his/her identification code and phone number;
2. Service provider forwards this information to DigiDocService. DigiDocService is a web service managed by CA that is used for communication between the server and mobile phone;
3. DigiDocService checks if the identification certificate is valid;

4. If the certification is valid, DigiDocService issues control code and user information (name and identification code) to the service provider via mobile operator. If the certificate is not valid, process is stopped.

5.-6. The user receives a pop-up message on the phone, which prompts them to enter their PIN if the control code on the service provider page matches the code in a pop-up message;

7. If the user enters the correct PIN onto the phone, the mobile operator passes the signature to DigiDocService;

8.-9. DigiDocService lets the service provider know that the user is authenticated and then the service provider automatically reloads a logged in screen [33]

- **Bank authentication**. The portal has made authentication via five different banks (SEB, Swedbank, Danske, Nordea, Krediidipank) available. Banks offer their own PIN calculators and password cards for authentication for their customers. When the user of an e-service has chosen to authenticate via bank, the user can choose whether to use the PIN calculator or password card for login. From the server logs of the state portal, it is not possible to determine which method users have used during individual logins. However, data about the usage of authentication methods in general from Swedbank shows that password cards are used more than PIN calculators. When choosing to authenticate either by PIN calculator or password card, 84% of the users use password card and 16% PIN calculators. Similar proportions have been observed by Krediidipank, where more than 80% of users authenticate themselves via password card.

  The PIN calculator generates a new unique OTP every time and the same password will never be used twice in a row. When a user wishes to authenticate, he/she uses the PIN displayed on the PIN calculator screen in addition to the normal password that is assigned to him/her. The authentication server knows the secret, token, stored in the user's PIN calculator. The server performs the same cryptographic function that the PIN calculator does. If the computer value matches the value that the user's PIN calculator displayed, the user is assumed to be in possession of the token [1], [35], [39], [53]. However, password cards have static

passwords. The password cards are plastic cards that have either 24, 36 or 72 passwords written in one side. While some banks issue a new password card once all the passwords have been used from the card, most banks reuse the passwords from the card repeatedly.

Generally, bank login works as follows (Figure 4):

1. The user inserts his/her username (and password if needed) to bank form;
2. Service provider sends authentication request to a bank;
3. The bank and service provider enter into an authentication services agreement during which they agree on authentication protocol and signature verification keys;
4. The bank server displays an *n*-digit challenge;
5. If the user authenticates with PIN calculator, the user inserts the code he/she knows to the PIN calculator. The matching response is calculated and it is displayed on a token. The user manually copies the response to the required field. When the user is using password card, the user inserts one of the passwords from the password card to the interface that is randomly asked by the bank server;
6. Bank asks permission to forward info to the service provider;
7. The user gives permission;
8. Logged in screen is reloaded [18], [21]

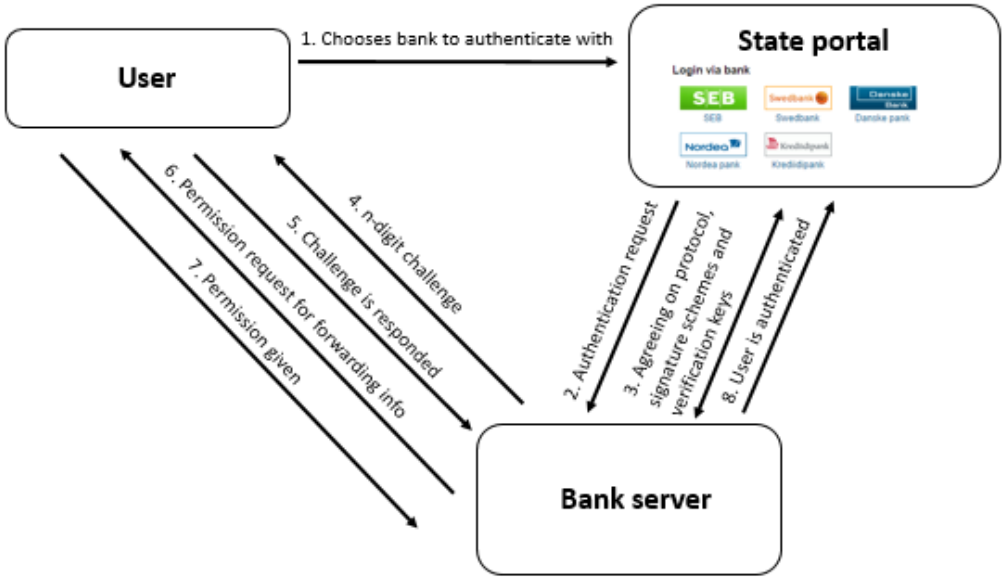

Figure 4. Authentication process with bank token.

3.3. Research measurements

In the present paper, the usable security of four different types of 2F authentication methods – ID card, mobile ID, PIN calculator and password card - are measured.

The research paper aims to test 4 hypotheses, and these are:

Hypothesis 1 (H1): Authentication methods differ from each other in their usability aspects;

Hypothesis 2 (H2): Authentication methods differ from each other in their security aspects;

Hypothesis 3 (H3): Authentication methods that score high in usability, score low in security;

Hypothesis 4 (H4): Users evaluate usable security of authentication methods rationally;

To test these hypotheses, usability and security dimensions are evaluated separately and they are evaluated of the perspective of the user. Usability of each authentication method is evaluated by measuring three usability dimensions: efficiency, effectiveness and satisfaction. Security of each authentication method is measured using attack trees.

Certain considerations about the scope of the present paper need to be mentioned:

1. The present paper researches only usable security of authentication function in the state portal and does not include the rollout of the authenticator. It is assumed that issuer of authenticator has issued it to the real and rightful owner;
2. It is assumed that organizations responsible for issuing authentication tokens are good-willed and do not have malicious intentions.
3. It is assumed that organizations responsible for managing authentication process are good-willed and do not have malicious intentions;
4. It is assumed that an attacker is rational;
5. Attack trees do not include breaking cryptographic algorithms as an attack method, since all organizations should be using 2048-bit RSA algorithms, which are almost impossible to break today. Breaking 2048-bit RSA would need $2^{103}/2^{61}$

x 350USD = 1 539 316 278 886 400 USD. Calculations are based on Schneier and Walker's views that 2^{61} operations (one processor year) costs around 350USD and security level of RSA 2048 is 103 [10], [11].

3.4. Usability measurements

3.4.1. Survey

An online survey was carried out which measured users' perceptions towards different authentication methods in general, meaning it was not state portal specific. In addition to the four authentication methods researched in the present paper, authentication via social networks was also included in the survey. Authentication via social networks is increasing in popularity, and this was added to the survey to discover which authentication methods users would prefer if they have the option to choose a method themselves. It was also important to determine how 2F authentication methods compare to other types of authentication methods.

The survey had 3 required questions for the users:

1. Which authentication method(s) you prefer using when logging in to an e- service;
2. How do you rate the usability of each authentication method (authentication methods were listed);
3. How you rate the security of each authentication method (authentication methods were listed);

When users had to rate usability and security, a 7-point Likert scale was used because that captures the intensity of the users' feelings best. Users had the option not to rate an authentication method, in case they had never used it. Users were also offered the option to comment freely about their feelings towards usability and security of each authentication method.

The Surveymonkey platform was used for conducting this survey and it was distributed through personal networks, public forums and e-mail lists. The required sample size for this survey was 385. Calculated for the population size of 1.4 million, with the confidence level 95% and confidence interval 5%.

3.4.2. Usability test

In order to understand the usability of the state portal specifically, and how using different authentication methods in the state portal compares to the usability ratings of authentication methods in general, a **usability test** was conducted.

There is no common agreement how big the sample size for usability tests should be. Nielsen and Virzi have argued that five is enough [29], [34]. This view has been opposed by many. For example, Bertaux argued that fifteen is the smallest acceptable size, Morse recommended at least six participants, while Kuzel recommended six to eight [17]. Macefield, who has analysed sample sizes for usability tests in depth has found that for comparative studies where statistically significant findings are being sought, a size of 8-25 participants is typically valid, with 10-12 participants being a sensible baseline [30].

For the present usability test, a sample size of 10 users for each authentication method was used. As every user was tested on 2 authentication methods, a total of 20 users were tested. This is in accordance with the recommended sample size for such a test [48].

Participants for the usability test were chosen among people who replied to the survey and who marked that they were interested in participating in it. All participants that were chosen for usability test had to meet two criteria:

1. They had used 2F authentication before;
2. They had to be able to log in by using at least two authentication methods;

All usability attributes - *effectiveness, efficiency* and *satisfaction* - were measured with usability tests and, where possible, compared to the logs of the state portal. Unfortunately, logs from the state portal did not make it possible to differentiate the various authentication methods. This is because some attributes about the user's logins are not stored.

Effectiveness - each authentication method was measured by the rate of successful logins to the system. General statistics about successful logins to the state portal were acquired directly from the state portal logs. However, it was not possible to determine from the logs, the different authentication methods used. Therefore, the success rate of each authentication method was only measured during usability tests.

Efficiency – it was measured with a time the user spent on authentication and with the number of clicks it took to achieve the goal. Authentication starts when the user is logged out and about to choose authentication method. The process ends when the user is successfully logged in and able to use a service.

The amount of time it takes a user to authenticate to the state portal was acquired from the state portal logs. However, it was not possible to differentiate, from the logs, the different authentication methods used. Therefore, the time it took to authenticate via each authentication method was measured during usability tests.

It is a given that the time required for authentication is related to the number of steps a user needs to take to authenticate themself. Therefore, in addition to measuring the time, the number of steps for the user to become authenticated was also taken into account. This information was gathered by conducting walkthroughs in the interface.

Satisfaction – For measuring satisfaction of using the state portal, the present research employed an attitude questionnaire during the usability test that used a 6-point Likert scale. The 6-point Likert scale was used in lieu of the usual 5 or 7-point scales in order to avoid any central tendency bias. As each participant had to do two tests, which might be tiresome for some users, it was important to avoid encouraging them to use neutral option for answers [2], [20], [50]. All questions which were used in the questionnaire were inspired from questionnaires used in previous work [12], [50] and they were fitted for the present research purpose.

In addition to using questionnaires, the present research measured users' brainwaves during the interaction to eliminate social desirability basis, and to see if the emotions users are feeling matched their feelings in questionnaire.

Brainwaves are produced by synchronized electrical pulses from masses of neurons communicating with each other, and they change according to what we are doing and feeling [51]. It is possible to spot when we are feeling relaxed, anxious, or when we concentrate. Brainwaves are measured in Hertz and they can be observed by using sensors and EEG tools. Measurement of brainwaves in the present research was done using NeuroSky's Mindwave EEG headset and Neuro Experimenter software. The Neuro Experimenter helps to capture brainwaves during the session in a way that makes it possible to later analyze them.

In the present paper we measured 3 waves – alpha 1, beta 1 and beta 2 to see what brainwaves were dominant during the authentication process.

Alpha (frequency 8Hz to 12Hz) are dominant during the resting state of the brain and represents relaxation [51], [55].

Beta (frequency 12Hz to 40 Hz) is present when we are alert, attentive, engaged in problem solving and they are allowing us to focus on tasks. When there is too much beta, it's a sign we are experiencing stress and anxiety. Beta brainwaves can be divided into two - high and low. Low beta (Beta 1) represents focus, active thinking, concentration, problem solving. High beta (Beta 2) represents high anxiety, excitement, alertness, nervousness, agitation and even panic state [51], [55].

Process of the usability test

The process of the usability test was described to the participants before the test. The process of the test was following:

1. An EEG headset was fitted on a participant and its connection with the software was checked;
2. The participant was asked to surf the web for 5 minutes, in order to get a baseline for brainwaves and in order to make him/her feel more relaxed;
3. After 5 minutes, the participant had to log in to eesti.ee portal by authentication method of their choosing. EEG headset's performance measuring and timer was started at the time when the participant opened eesti.ee webpage;
4. After logging in, the participant had to find European Health Insurance Card tab under Services page. The test finished when the participant clicked on the tab;
5. After the test, the participant was asked to fill in attitude questionnaire which measured their satisfaction with the process.
6. After filling in the questionnaire, the participant was given a 10-minute break;
7. After the break, steps 2-5 were repeated;

3.5. Security measurements

Security of each authentication method was determined by using attack trees. Attack trees were created from the attacker's perspective. All the possible attacks (goals) were listed and all attributes were assigned to the leaf nodes. Metrics used in the present research were **probability** and **impact**, which were used to calculate overall **risk** level [15], [22], [42]. These metrics were chosen because they help to measure how secure each authentication method is, in the most accurate way.

The probability *(P)* of success represents the attacker's probability of successfully completing the attack at a specific node. Probability is a number between zero and one, where zero is the least probable and one the most probable. Probabilities are usually determined by using past data or by estimation [15], [47]. Table 1 shows the OWASP probability scale with numerical range that was used in the present paper.

Table 1. OWASP probability scale.

Probability	Numerical range
Low	0 to < 1 0.3
Medium	0.3 to < 0.6
High	0.6 to < 1

The impact *(I)* defines how the system will be affected if the attacker is successful at that node. When we talk about impact, we have to take in consideration both technical and business impact and estimate the magnitude of them to the system if it is exploited. Technical impacts are related to traditional security areas such as confidentiality, integrity, availability. Business impact is related to what is important and critical to business in general [36].

Different researchers have used different metrics to assign impact. NIST magnitude of impact ranges from low (10) to high (100), while Edge and Weiss used scale ranged from one to ten [15], [47]. Ingoldsby has given monetary values to impact. The most widely used metric, which is also used in the present paper, is assigning impact values low, medium or high, which correspond to numeric scale 0 to 1 [23], [40]. Table 2 gives an

overview of impact definitions [14], [36] used in the present paper. The impact of each node in the attack tree was discussed through with experts in the field, employees of Sertifitseerimiskeskus and Estonian Information System Authority.

Table 2. Impact definitions.

Impact	Numerical range	Impact Definition
Low	0 to < 0.3	Minimal impact to system. Easily detected and/or repaired Technical impact: data slightly corrupted, minimal non-sensitive data disclosed; minimal secondary services disrupted; Business impact: one user's privacy is violated; no damage to the reputation; no effect to annual profit
Medium	0.3 to < 0.6	Moderate impact to system. Requires non-trivial effort to detect and/or repair Technical impact: minimal critical data and/or extensive non-sensitive data disclosed; minimal primary services; Business impact: minor effect to annual profit; minimal damage to the reputation; privacy of hundreds of users violated;
High	0.6 to 9	Severe impact to system. Considerable effort required to detect and/or repair damage Technical impact: extensive critical data disclosed; extensive primary services interrupted; data corrupted; Business impact: brand damage; significant effect to annual profit;
	1.0	System completely compromised, inoperable, or destroyed

The risk *(R)* shows how secure each authentication method is, since risk is a function of the probability of an attack being successful and the resulting impact of this attack [8], [15], [32], [47]. After values have been assigned to nodes, a value of risk can be therefore calculated by using the formula:

Risk = probability x impact

When values of risk levels are determined, it is possible to see how secure each authentication method is and how they compare with each other. Table 3 shows OWASP risk severity that is based on impact and probability. The table gives a good visual

overview on how the combination of probability and impact help to determine if the risk level is low, medium, high or critical.

Table 3. OWASP Risk severity.

		Impact		
		LOW	MEDIUM	HIGH
Probability	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium

3.5.1. Calculations of nodes

Slater, Jürgenson et al., Edge et al. all agree that to determine an attribute value for a scenario of attack tree, the bottom up approach is best to use. This means attribute values are assigned only for the leaf nodes because they are the only nodes the attacker has some control over. Refined nodes get their values computed from child node values by applying a set of rules [14], [26], [43]. Table 4 describes rules that are used to calculate AND and OR value nodes in the present paper. This table is, in great extent, based on a rules table used by Edge et al.

Table 4. Rules for attack trees.

	AND nodes	**OR nodes**
Probability	$\prod_{i=1}^{n} prob_i$	$1 - \prod_{i=1}^{n} (1 - prob_i)$
Impact	$1 - \prod_{i=1}^{n} (1 - impact_i)$	$Max_{i=1}^{n} impact_i$

$prob \in (0,1]$, $impact \in [0,1]$; n = number of child nodes

- When we talk about probability, in AND relationships, every action the attacker takes has to be successful in order for the parent node to be successful. Therefore, the probabilities of the child nodes are multiplicative which lowers the total probability of the parent node. In OR nodes, the approach is different since we

must take into account that elementary attacks contribute to the success probability [14], [23], [26], [27].

- In OR nodes, the attacker goes for maximum impact because we assume attacker is rational. In AND nodes, elementary attacks contribute to the impact and therefore we have to consider impact of them in determining parent node [14], [23], [26].
- Risk for each node is calculated separately by using the above mentioned formula, probability x impact.

4. Results

4.1. Usability

4.1.1. Survey

Survey received 393 responses. 57% respondents said that if they can choose, they prefer to authenticate with ID card. 43% would prefer to authenticate with mobile ID. Detailed survey results can be found form Appendix 1.

The online survey results showed that users evaluate social network authentication as the most usable – average mean 5.76 out of seven. However, when users have to authenticate into e-services with two factor authentication method, they find ID card the most usable to use - average usability mean 5.54 out of 7 on the Likert scale. Mobile ID fell a little behind, with an average mean of 5.51 out of 7. Authentication via bank got the lowest average means – the PIN calculator has 5.39 and password card has 5.42 out of 7. Table 5 shows the mean usability results of the survey and number of responses.

Table 5. Usability results of the survey.

	Mean	Standard Deviation	N
Social networks	5.76	1.79	325
ID card	5.54	1.72	383
Mobile ID	5.51	1.87	306
Banks password card	5.42	1.69	367
PIN calculator	5.39	1.71	363

N = number of responses

When survey participants were asked freely to comment on what makes an authentication method usable vs unusable, certain usability attributes were mentioned repeatedly. 80 participants said that the number of clicks is important in making an authentication method usable. Meaning, the smaller the number of clicks, the more usable the method

is. This is closely related to the speed of authentication. 54 participants mentioned speedy authentication is more usable. 71 participants mentioned that having a device in their disposal on a regular basis by default (built in ID card reader, mobile ID) makes authentication more usable. This correlates to 23 participants' opinion that connecting ID card reader with a computer and setting up authentication in other ways decreases usability.

4.1.2. Usability test

Efficiency

The logs from the state portal revealed that the percentage of unsuccessful authentications is 4%. During the usability tests, most unsuccessful authentications happened during authenticating with password card – 4 unsuccessful logins out of 10. PIN calculator and ID card both had 2 unsuccessful logins and mobile ID only had 1.

In all cases of unsuccessful logins in usability test, users had entered the wrong PIN or password. From the brainwave results it was possible to see, that only in 3 instances out of 9 users stress level increased as a result, which shows that unsuccessful logins do not necessarily increase the stress level of users.

Effectiveness

According to logs from the state portal, average authentication time is 61 seconds. Usability test results showed that ID card offered the fastest authentication – average authentication time was 57 seconds, and the slowest authentication method was the password card at 76 seconds. In table 6 it is possible to see average login times and the number of steps the user needs to make when authenticating. The number of steps with description for each authentication method can be found in Appendix 2.

Table 6. Login time results and number of steps.

	Mean in seconds	Number of steps
ID card	57	6
Mobile ID	65	5
PIN calculator	67	9
Password card	76	8

From the results it is possible to see that the number of steps user needs to take, does not make the process of authentication necessarily slower. For example, authentication with a PIN calculator takes 9 steps but only 65 seconds, while authentication with a password card requires 8 steps but takes on average 76 seconds. When we combine data of efficiency and effectiveness, it is possible to see that number of unsuccessful logins influences the average time of authentication. For example, 4 mistakes were done when authenticating with a password card. Even though the password card did not require the most number of steps, the average time of authentication was much longer than in any other method. Additionally, though mobile ID takes only 5 steps, it still is not significantly faster than PIN calculators, which require users to take 9 steps.

We see that efficiency of an authentication method is not a straight forward criteria. It depends on several factors – number of mistakes the user is making, errors, how long it takes to establish a session with the server, how long it takes for DigiDocService to check if certificate is valid, etc.

Satisfaction

Results of usability test differed from the survey results somewhat. Results in length can be found from Appendix 3. Participants of usability test rated mobile ID as the most satisfying to use with average mean of 5.49 out of 6, and password cards the least satisfying to use, with an average mean of 4.91. Mean usability results for three methods can be found in table 7.

Table 7. Usability results of usability test.

	Mean	Standard Deviation	N
ID card	5.38	0.28	10
Mobile ID	5.49	0.34	10
PIN calculator	5.28	0.26	10
Password card	4.91	0.43	10

N = number of participants

Satisfaction attitude questionnaire measured 13 attributes for each authentication method. Results of questionnaire can be seen in table 8.

Table 8. Usability attribute scores.

	ID card	Mobile ID	PIN calculator	Password card
Convenient to use	5.4	5.6	5.3	5.3
Speed of using device	5.6	5.4	4.9	4.8
Degree of enjoyment	5.3	5.4	5.1	4.8
Would use device again	5.6	5.7	5.2	5.0
User-friendliness	5.5	5.4	5.3	4.9
Trustworthiness	5.6	5.7	5.0	5.3
Easy to use without instructions	5.0	5.9	5.5	4.4
Didn't demand high concentration	4.4	4.8	5.3	3.8
Stress free	5.8	5.8	5.5	4.9
Didn't cause frustration	5.8	5.7	5.7	5.3
Not complicated	5.5	5.6	5.7	5.0
Degree of security	5.4	5.6	5.1	5.0
Easy to use for the first time	5.0	4.8	5.0	5.4

The ID card was characterized with positive attitudes (above 5 on the 6-point scale) towards usability for 12 (92%) out of 13 attributes. Participants considered the experience stress and frustration free, thought it was very trustworthy and would use this authentication method again in the future. What users did not like about ID card authentication was that it needed more concentration and instructions and was not considered easy to use for the first time.

Mobile ID was characterized by positive attitudes towards usability for 11 (85%) out of 13 attributes. Participants rated the highest attributes related it being stress free and easy to use without instructions. Similar to ID cards, mobile ID authentication received the lowest scores in attributes related to needing more concentration. Users thought that mobile ID authentication was not so easy for first time usage.

Participants characterized the PIN calculator with positive attitudes towards usability in 12 (92%) out of 13 attributes. The PIN calculator was considered easy to use and it

offered frustration free experience. PIN calculator scored low in speed, trustworthiness and ease to use for the first time.

The password card was characterized by positive attitudes towards usability for 7 (54%) out of 13 attributes. Password cards were considered convenient to use, trustworthy, frustration free and it was easy to use for people who used it for the first time. PIN calculator shortcomings were that it needed a lot of concentration and it was not easy to use without instructions.

Brainwave results

Participants in usability tests have a tendency for social desirability bias, meaning that they try to portray themselves in a more favorable light. Thus, their score was checked to determine if it matched with the feelings they had during the experience [20]. This was accomplished by checking if brainwave results match their questionnaires answers on usability on convenience, concentration, stress and frustration.

Neuro Experimenter program that was used for measuring brainwaves represents a ratio of the performance over the baseline for each wave type. Baseline is 1 and if performance either falls below or above 1, it shows that the particular emotion was more or less prevalent in a participant than normally. Table 9 shows the results of average performance results for brainwave measurements.

Table 9. Brainwave measurements.

	Alpha 1	**Beta 1**	**Beta 2**
ID card	0.97	1.13	0.92
Mobile ID	1.29	1.21	0.97
PIN calculator	0.98	1.11	0.97
Password card	1.08	1.23	1.01

Convenience can be measured with alpha 1. Alpha 1 is related to relaxation and calmness. We see that mobile ID users' performance in this category is significantly above baseline. Mobile ID users' average mean convenience was also the highest. For other type of

authentication, the average mean was similar and we see from the brainwave performance that it is indeed close to baseline.

Concentration can be measured with beta 1. From the brainwave results, we see that all authentication methods involved significant concentration. Authenticating by password card (performance 1.23) and mobile ID (performance 1.21) required the most concentration. When we observe means of participants scores, we observe that they have considered those two methods to be concentration demanding methods alongside with ID card.

Frustration and stress can be measured with beta 2. The average mean showed us that the most stressed and frustrated users were the password card users - whereas the least were ID card and mobile ID users. However, it was possible to see from the average means that none of the authentication method caused participants a lot of stress or frustration. From the brainwave performance we see that level of stress and frustration was almost the same as baseline results for each authentication method. That also matches the average means.

4.1.3. Summary of usability dimensions

We see that the overall usability test results differ from the survey results slightly – mobile ID is considered more usable than ID card by usability test participants. Results vary because, during the usability test the users evaluated authentication methods usability in the state portal specifically, while in the survey the users evaluated their attitude towards an authentication method's usability in general. However, in both cases we see that there is little difference in terms of satisfaction between authentication methods. We also see from the usability test results that ID card, mobile ID and PIN calculator are all considered very usable in terms of satisfaction.

Usability depends on several factors and is not straight forward to measure. However, from the results of usability dimensions there are certain conclusions that we can draw (table 10).

Table 10. Summary of usability attributes

	Average mean	Time for authentication in seconds	Number of steps	Number of mistakes
ID card	5.38	57	6	2
Mobile ID	5.49	65	5	1
PIN calculator	5.28	67	9	2
Password card	4.91	76	8	4

We can see that mobile ID and ID card both are considered highly usable by users. These methods offer speedy authentication with few steps and do not cause many mistakes. The PIN calculator offers good usability, but not as good as mobile ID and ID card. The PIN calculator takes a bit longer to authenticate and involves over 60% more steps for the user. Using a PIN calculator is also not as satisfying for users. Password cards perform the worst in terms of usability. Password cards are not highly ranked in terms of satisfaction, they take many steps and a long time to authenticate and they are the most mistake-prone among the authentication methods researched.

4.2. Security

4.2.1. Survey

Online survey results showed that users evaluate ID card authentication as the most secure – average mean was 6.34 out of seven. Authentication via mobile ID and via bank was believed to be similar in terms of security. Mobile ID security mean 5.74 was slightly higher than PIN calculator's 5.71. The password card was considered a bit less secure, with an average security mean 5.66 out of 7. Even though social networks were considered high in their usability, they scored very low in security – average mean was 2.26 out of 7. Table 11 shows the mean security results of the survey and number of responses.

Table 11. Security results of the survey.

	Mean	Standard Deviation	N
Social networks	2.26	1.43	356
ID card	6.34	0.97	379
Mobile ID	5.74	1.49	319
Banks password card	5.66	1.32	366
PIN calculator	5.71	1.39	308

Survey participants were asked freely to comment on what makes an authentication method secure. Even though selection of security factors that was mentioned was wide, a couple of common themes came up. 55 respondents mentioned that using 2F to authenticate makes authentication more secure. 43 people believed that issuer of authenticator makes authentication secure, and those participants had very strong confidence in the strength and good-will of banks and the state. This is reinforced with 25 respondents who did *not* believe that big corporations, such as Google or Facebook, can keep their data and authentication credentials secure. 22 respondents believed that knowing their password by heart is already making authentication secure enough. 18 respondents thought that security is subjective and there is no one answer for what makes authentication secure. 11 respondents thought that internet itself is insecure and therefore nothing can be secure.

4.2.2. ID card

Attack tree of compromising ID card authentication is shown in figure 5.

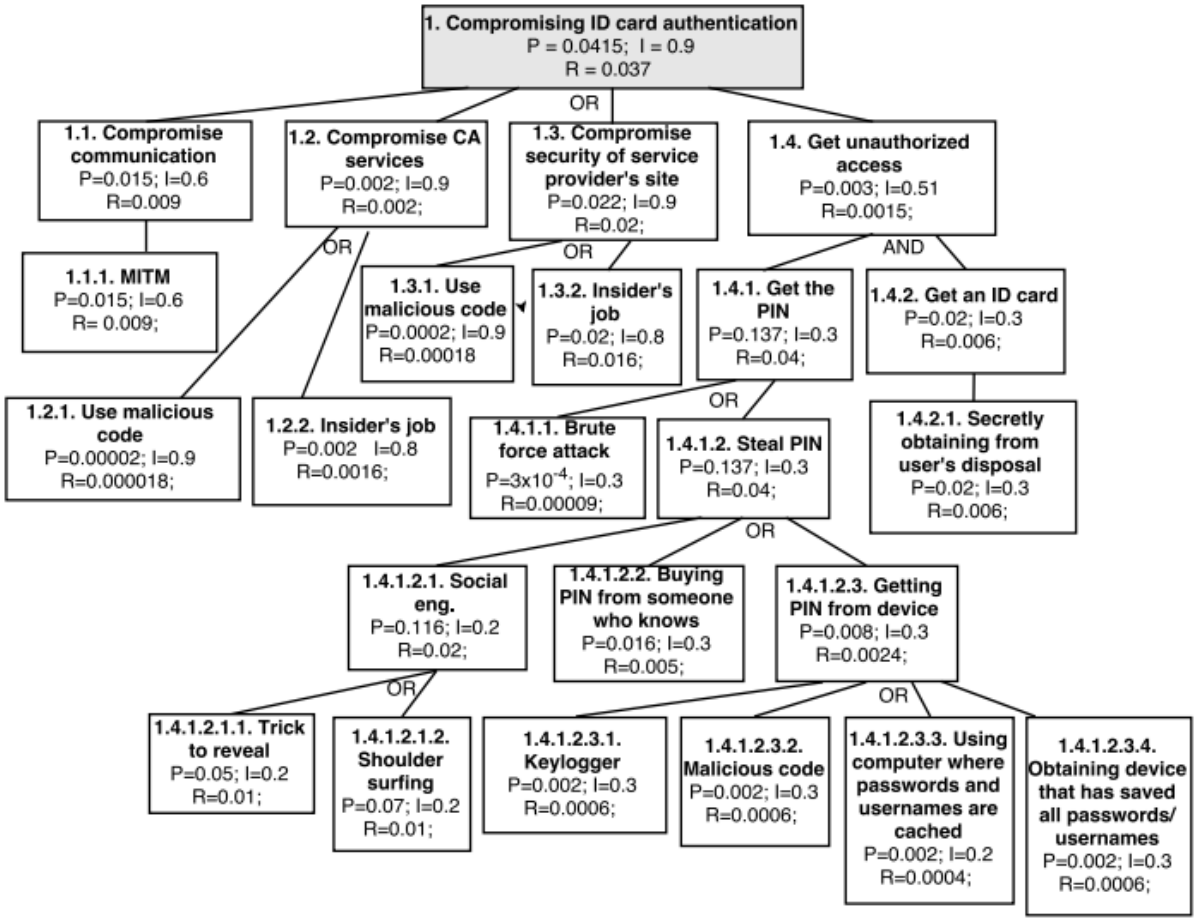

Figure 5. Attack tree of ID card authentication.

It is possible for the attacker to compromise ID card authentication in four different ways – compromising communication, compromising systems of CA, compromising security of service provider or get an unauthorized access. This OR relationship gives our ultimate goal values of:

P = 0.0415; I = 0.9; R = 0.037;

Explanation of attack vectors and reasoning of the values of P:

- *1.1. Compromise communication* – a difficult, but theoretically possible, way to get an access to the authentication credentials is to compromise the communication between the client and the server.

- *1.1.1 MITM* – in man-in-the-middle attack, the attacker is between the server and the client and he is altering the communication between the two. It is even possible for the

attacker to change digital certificates sent over SSL connection. However, in the end of the session establishment of ID card authentication, the whole package of messages is signed with private key by both parties. If those keys do not match with keys individual messages were signed with, the connection is dropped. That eliminates MITM attack in one way. However, there is always an option that there is a vulnerability in SSL protocol itself, which still makes MITM attack possible. Reasoning for values of P:

P: 0.015. The probability that adversaries have succeeded to gain control over the connection between the servers is 0.15[7]. However, in case of critical infrastructures, such as CA, the probability is lower, because of above mentioned signing of messages with private keys. The probability in case of CAs and bank OTP is 0.015.

- *1.2. Compromise CA services* - an attack can be launched against CA as this is the organization that verifies the validity of certificates.

- *1.2.1 Use malicious code* – malicious code can be hidden in CA's side to compromise or corrupt systems of CA. That could corrupt the validity of certificates or disable certificate validation service. Reasoning for P:

P: 0.002. The probability of exploiting a bug in an operating system or hardware and getting access to a system is ≈ 0.002 [7]. However, in critical infrastructure systems, such as CA, the probability is much lower because systems are highly controlled and monitored, so the probability there is estimated to be 0.00002. Service provider and third party's systems are also controlled and monitored much more than they would be at regular home user's, but not as highly as they are in critical infrastructure systems, so the probability is 0.0002.

- *1.2.2. Insider's job* – an insider can be hired to compromise the systems of CA in a way that certificates are corrupted or the availability of certificate validation service is disabled. Reasoning for value of P:

P: 0.02. The probability of at least one insider incident of sabotage of systems, network or data to take place within 2 years in midsize/large organization is 21% [31]. However, Estonia is a very small country and an insider who is helping to sabotage systems has more to lose than a person in the same position in a bigger country. Therefore, it is assumed that the probability is 10% of average world statistics. The probability is even

lower in organizations that manage critical infrastructures, such as CA and also in a bank. The probability there is even lower – 0.002.

- *1.3. Compromise security of service provider's site* – an attack can be launched against service provider.

- *1.3.1. Use malicious code* – Malicious content is installed in service provider's site or systems. Malicious content can take an advantage of well-known vulnerability of a web browser. Reasoning for value of P is the same as in 1.2.1.

- *1.3.2. Insider's job* – Reasoning the same as in 1.2.2.

- *1.4. Get unauthorized access* – If the attacker has obtained the ID card, he can use different ways to find out PIN1 of the ID card in an attempt to open authentication key.

- *1.4.1.1. Brute force attack* – One way to get the PIN1 is to use brute force. The attacker can try different PIN1 combinations in an attempt to authenticate. Reasoning for value of P:

P: 0.0003. PIN1 can be entered incorrectly three times before it is locked. PIN1 can be minimum of 4 numbers long, which means there are at least 10^4 possible combinations to guess the PIN1.

- *1.4.1.2.1. Social engineering* – Social engineering techniques can be used to find out PIN1 that the user is using.

- *1.4.1.2.1.1. Trick to reveal* - users can reveal passwords and PIN numbers if they are tricked. For example, an attacker can pretend to be a representative of the service provider. Reasoning for value of P:

P: 0.05. 5% of the users respond to request for personal data when it is asked from them with spoofed e-mail, so it can be assumed that the similar percentage of people would reveal their secrets when asked in other ways [18]

- *1.4.1.2.1.2. Shoulder surfing* - When credentials are entered to web interfaces in public space, most users do not hide this activity well. This makes it possible for others to see their credentials. Value of P:

P: 0.07. Survey done in the UK in 2012 showed that 71% of people were able to see or read what someone was working on in a public place [19]. However, in Estonia, the awareness of possibility of shoulder surfing is higher thanks to awareness programs according to analyst in Estonian Information System Authority, which makes the probability much lower. It is assumed that the probability is 10% of what it is recorded in the UK.

- *1.4.1.2.2. Buying PIN from someone who knows* - Often users share their PINs and passwords with other people they know. Since people can be bribed for certain amount of money, it is possible to find a person who knows someone else's PIN1 and bribe them for revealing it. Reasoning for value of P:

P: 0.016. About 33% of people can be bribed for 46 000 EUR [7]. However people awareness of disclosing their PINs is high in Estonia, plus finding a person who knows the PIN is very difficult. That is why it is assumed that even though 33% of people can be bribed, the chance of finding the person who knows PIN is maximum 50% of that.

- *1.4.1.2.3.1. Keylogger* – If a smartcard reader does not have a PIN pad on it, the PIN1 needs to be entered from the keyboard. When the PIN1 is entered from the keyboard, the operating system has access to the PIN1. If the computer is infected with malicious software, the attacker can get the access to the PIN1 with a help of malware called keylogger [96]. Reasoning for value of P is the same as in 1.3.1.

- *1.4.1.2.3.2 Malicious code* - It is possible that malicious content is installed in user's device which can obtain the users credentials. The device can be compromised when malicious code is sent to a user, which executes malicious software when opened. The malicious hidden code can capture information, such as username and PIN codes and can regularly send this information to an attacker. Reasoning for value of P is the same as in 1.3.1.

- *1.4.1.2.3.3. Using computer where passwords and usernames are cached* – Some browsers can cache PIN1 after an active ID-card session if the user did not log off after their session and/or does not close the browser after the session. As a result of this it is possible to authenticate into other e-services without actually entering PIN1 again. Reasoning for P:

P: 0.02. Probability is similar to the probability of getting an access to a device that belongs to someone else [37]. See 1.4.2.1.

- 1.4.1.2.3.4. Obtaining device that has saved all passwords/usernames – Some devices, such as Hewlett Packard (HP) laptops with fingerprint reader, make it possible to authenticate into e-services without entering PIN codes. This is caused by HP ProtectTools Security Manager Software, which automatically saves PIN1 and PIN2 at first authentication [97]. However, such software is not only limited to HP computers. Reasoning for the value of P is the same as in 1.2.1.

- 1.4.2. Get an ID card – Together with PIN1, an attacker needs to have an ID card in his disposal in order to be able to authenticate on user's behalf.

1.4.2.1. Secretly obtaining from user's disposal – ID card can be stolen from person's disposal deliberately. ID cards are often kept in wallets with other documents or just left somewhere where someone can take it. Reasoning for P:

P: 0.02. Wallets can be as easy to steal as mobile phones. According to Home Office statistics the theft of mobile phones has been relatively stable over the last decade, and the chances of a person becoming a victim of phone theft has not exceeded 2% [37].

4.2.3. Mobile ID

Attack tree of compromising mobile ID authentication is shown in Figure 6.

It is possible for the attacker to compromise mobile ID authentication in five different ways – compromising communication, compromising systems of CA, compromising security of service provider, compromising mobile service provider's system or getting an unauthorized access. This OR relationship gives our ultimate goal values of:

P= 0.105; I = 0.9; R = 0.094;

Explanation of attack vectors that has not been described so far and reasoning of the values of P:

2.1. Compromise communication – Reasoning the same as in 1.1.

2.2. Compromise CA services - as in 1.2.

2.3. Compromise security of service provider's site - as in 1.3.

2.4. Compromise mobile-ID service provider's systems – as in 1.3.

2.5.1.1.1. Brute force attack – as in 1.4.1.1.

2.5.1.1.2.1. Social engineering - as in 1.4.1.2.1.

2.5.1.1.2.2. Buying PIN from someone who knows - as in 1.4.1.2.2.

2.5.1.1.2.3.1. Malicious code – as in 1.3.1.

2.5.1.1.2.3.2. Keylogger – as in 1.4.1.2.3.1.

2.5.1.1.2.3.2. Using device faults of the device – The attacker can exploit hardware vulnerability. Reasoning for P the same as in 1.2.1.

2.5.1.2. Get the phone with SIM card – as in 1.4.2.

2.5.2. Send an authentication request to list of users- when authenticating with mobile ID, the users identification code and phone number must be entered on the login page. It is not difficult to discover the identification code and mobile phone numbers of individuals. Thus it is possible for an attacker to initiate an authentication request and hope that the users will accidentally enter his/her credentials on their mobile phone, when control code is sent. This would make it possible for an attacker to authenticate himself to the system. Reasoning for value of P is the same as in 1.4.1.2.1.1.

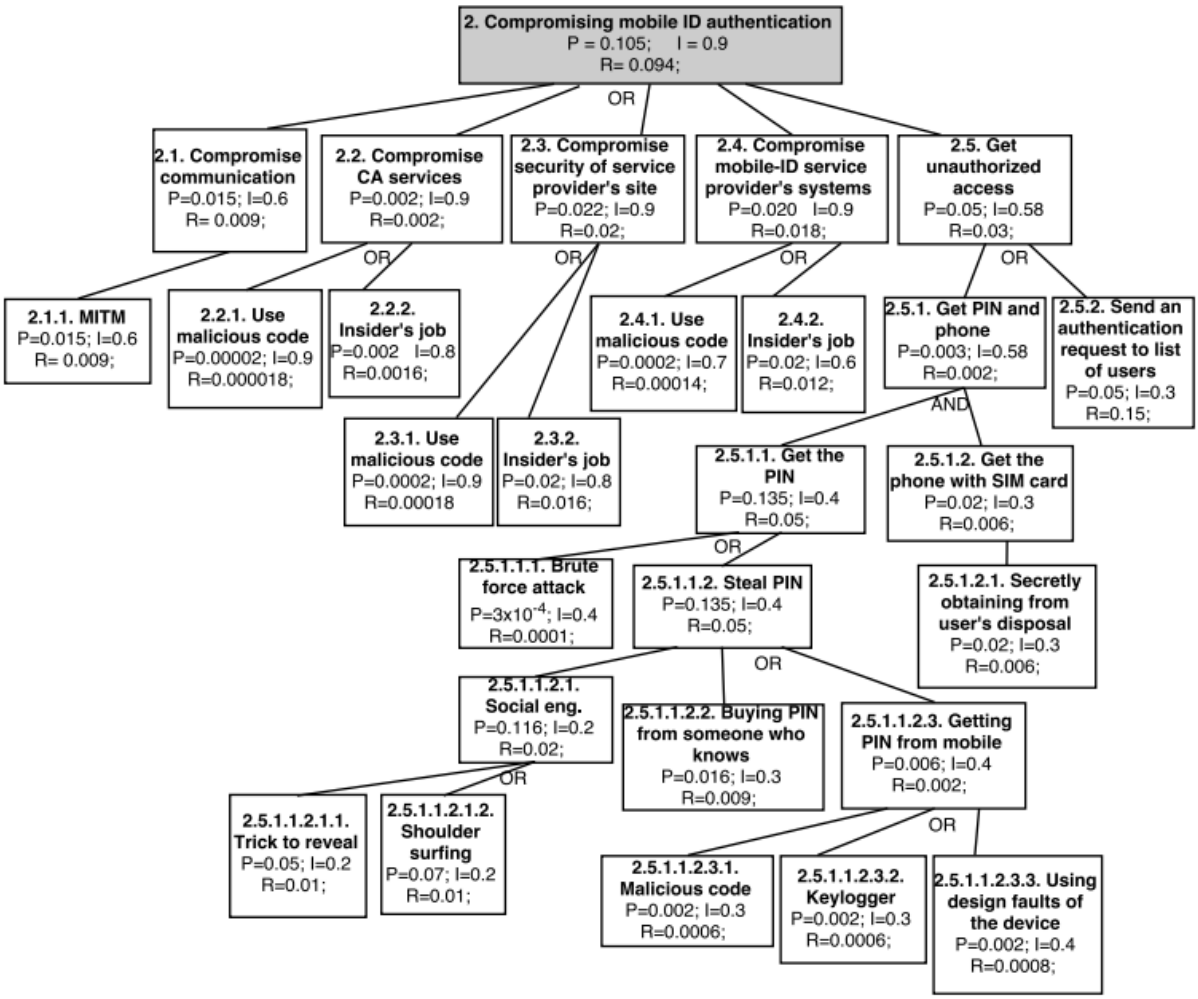

Figure 6. Attack tree of mobile ID authentication.

4.2.4. PIN calculator

It is possible for the attacker to compromise PIN calculator authentication in four different ways – compromising communication, compromising bank systems, compromising security of service provider or getting an unauthorized access. This OR relationship gives our ultimate goal values of:

P= 0.0853; I = 0.9; R = 0.077;

Explanation of attack vectors that has not been described so far and reasoning of the values of P:

- *3.1.1. MITM attack* – Reasoning for value of P is the same as in 1.1.1.

- *3.1.2.1. Use convincing website* – user is directed to a website, that looks like a real website, but which is not. An attacker can direct the user to a malicious site and steal his/her credentials from there when entered. Reasoning for value P is the same as in 1.4.1.2.1.1.

- *3.2.1 Use malicious code* – Value of P is the same as in 1.2.1.

- *3.3. Compromise security of service provider's site* - as in 1.3.

- *3.4.1.1.1. Guess username* – The attacker needs to guess the username. Reasoning for value of P:

P: 0.00001. There is no limitation how many times username can be entered incorrectly. Username can be a minimum of 5 numbers long (length depends on the bank), which means there is 10^5 possible combinations.

- *3.4.1.1.2. Guess PIN* - The attacker needs to guess the PIN. Reasoning for values of P:

P: 0.00003. It is possible to enter the PIN incorrectly three times, after that the system locks it. PIN can be a minimum of 5 numbers long (length depends on the bank), which means there is 10^5 possible combinations.

- *3.4.1.2.1.1. E-mail phishing* - the user is sent an e-mail that is asking them to enter their credentials to a certain website or a form. Value of P is the same as in 1.4.1.2.1.1.

- *3.4.1.2.1.2. Trick to reveal* – as in 1.5.2.2.1.1.

- *3.4.1.2.1.3. Shoulder surfing* – as in 1.5.1.2.1.2.

- *3.4.1.2.2. Buying username and PIN from someone who knows* - as in 1.4.1.2.2.

- *3.4.2. Get PIN calculator* - as in 1.4.2.

Attack tree of compromising PIN calculator authentication is shown in Figure 7.

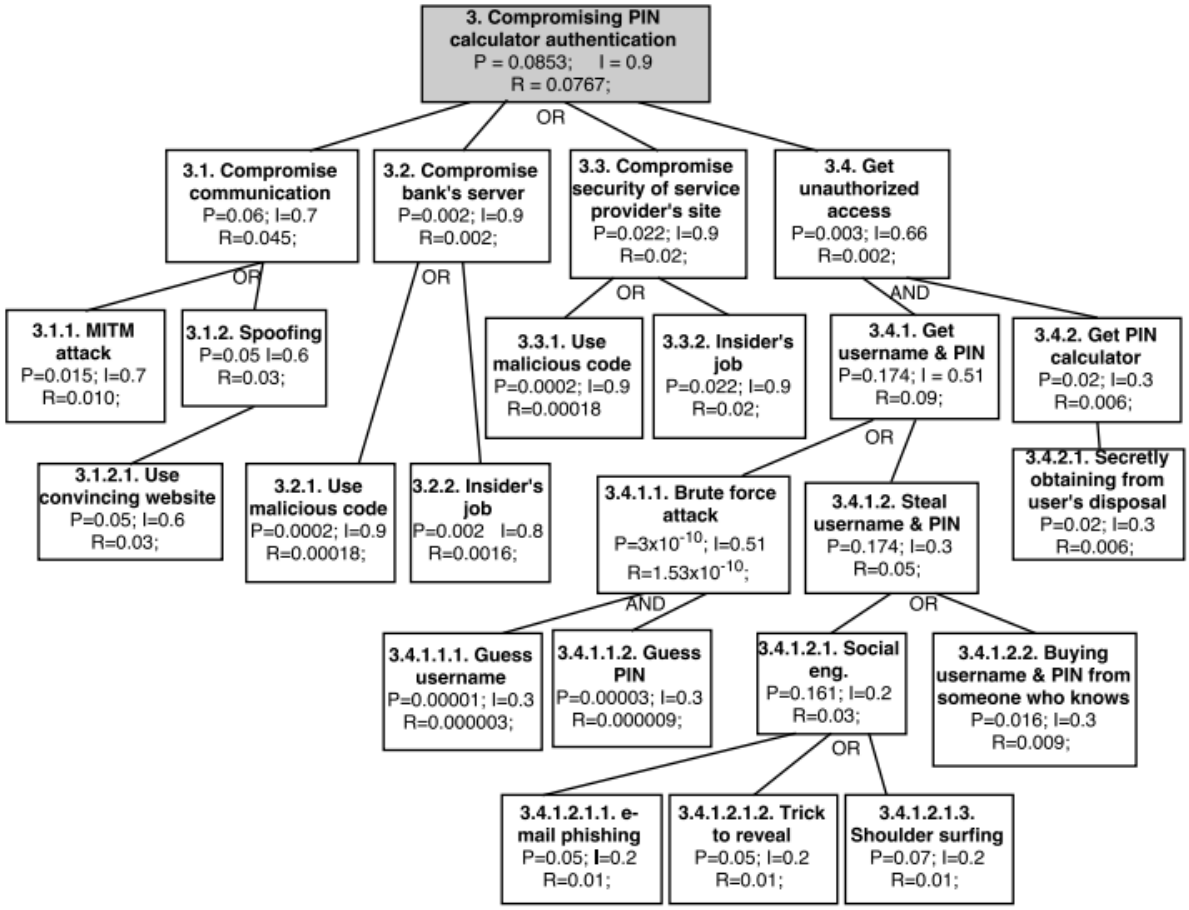

Figure 7. Attack tree of PIN calculator authentication.

4.2.5. Password card

It is possible for the attacker to compromise password card authentication in four different ways – compromising communication, compromising bank server, compromising security of service provider or getting an unauthorized access. This OR relationship gives our ultimate goal values of:

P= 0.258; I = 0.9; R = 0.232;

Explanation of attack vectors that has not been described so far and reasoning of the values of P:

- 4.1. Compromise communication - as in 3.1

- 4.2. Compromise bank server - as in 3.2.

- *4.3. Compromise security of service provider's site* - as in 1.3.

- *4.4.1.1. Brute force attack* - as in 3.4.1.1.

- *4.4.1.2. Get password card* – It is easier to obtain password card than it is to steal other type of tokens. With password card it is enough to take a picture of the card to get an access to all passwords and taking the picture takes just a second and be easily done everywhere. It is assumed that it is 5 time easier to get a hold of the password card than it is to obtain other tokens (see also 1.4.2.1.)

- *4.4.2.1. Get password card* - as in 4.4.2.1.

- *4.4.2.2.1. Social engineering* - as in 3.4.1.2.1.

- *4.4.2.2.2.1. From organized crime* - It is possible that credentials have been acquired by hackers who have sold them in a black market. The attacker can buy them if needed. Reasoning for value of P:

P: 0.43. 43% of companies had a data breach in 2013 [49]

- *4.4.2.2.2.2. Buying username and password from someone who knows* - as in 1.4.1.2.2.

- *4.4.3. Get username and password from device* - as in 1.4.1.2.3.

Attack tree of compromising password card authentication is shown in Figure 8.

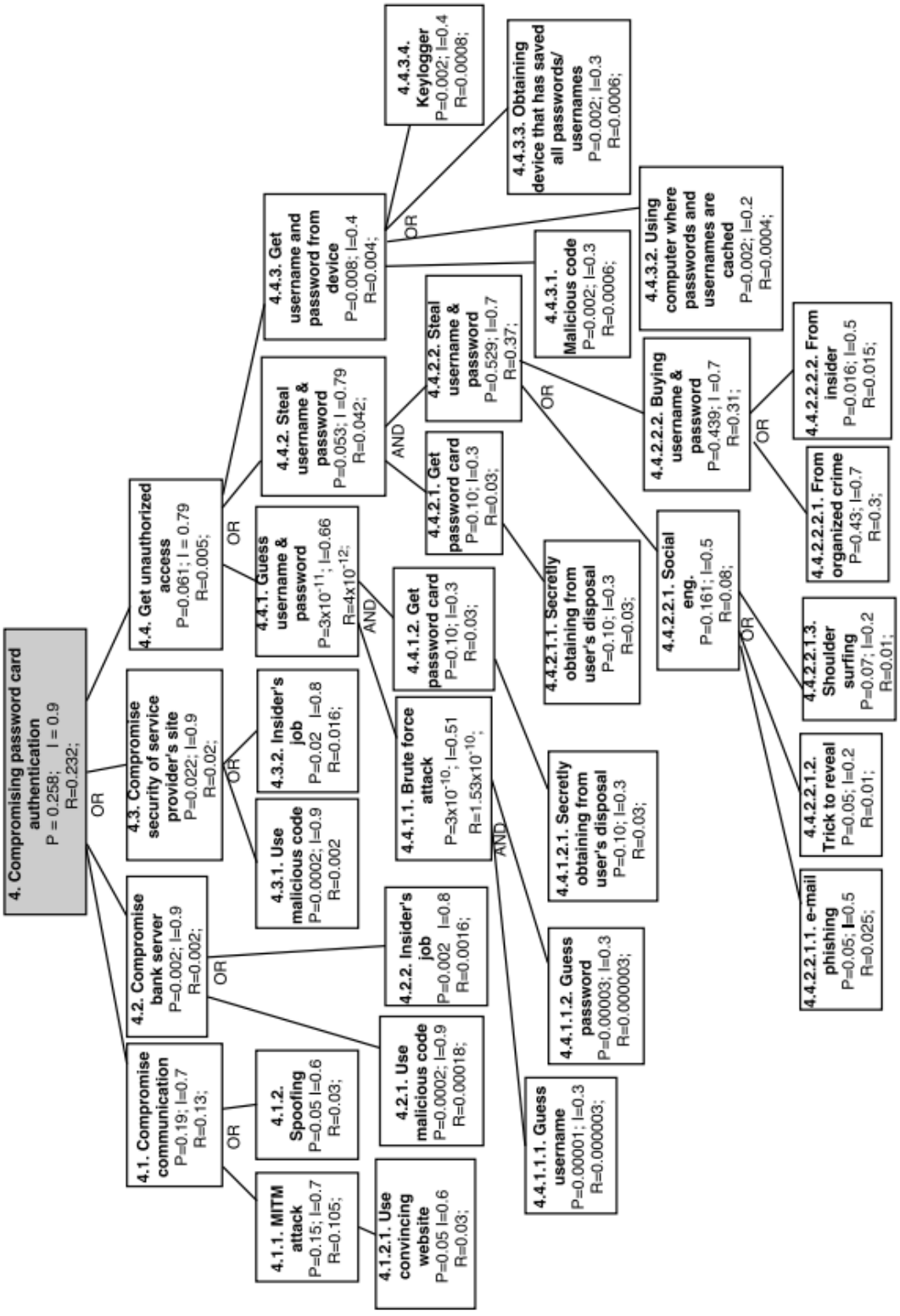

Figure 8. Attack tree of password card authentication

4.2.6. Summary of security dimensions

From the analysis of attack trees we see that ID card is by far the most secure with the risk of 0.037. PIN calculator has the second lowest risk from the remaining three authentication methods – 0.077. Mobile ID falls a bit behind of PIN calculator and has the risk on 0.094. Password card has the highest risk, 0.232, which is more than 6 times higher than ID card's and more than twice higher than mobile ID's.

Probability of compromising each authentication methods is low, but impact is high, which makes overall risk level medium for each method. If the attacker is successful in compromising any of the authentication methods, it would not only take considerable effort to repair the damage, it would have significant negative damage to the trust of e-services and e-state in general. All values of security dimensions can be found from Table 12.

Table 12. Summary of security dimension values.

	P	**I**	**Risk**	**Risk Level**
ID card	0.0415	0.9	0.037	Medium
Mobile ID	0.105	0.9	0.094	Medium
PIN calculator	0.0853	0.9	0.077	Medium
Password card	0.258	0.9	0.232	Medium

5. Conclusions

The aim of the present research was to find out which 2F authentication method used in Estonia works best, in terms of usability and security. State portal, eesti.ee was used as the case study. Summary of results of usability and security dimensions that were measured in the present research are shown in table 13.

Table 13. Values of usability and security dimensions.

	Satisfaction mean (out of 6)	**Time for authentication in seconds**	**Number of steps**	**Number of mistakes**	**Probability**	**Impact**	**Risk**
ID card	5.38	57	6	2	0.0415	0.9	0.037
Mobile ID	5.49	65	5	1	0.105	0.9	0.094
PIN calculator	5.28	67	9	2	0.0853	0.9	0.077
Password card	4.91	76	8	4	0.258	0.9	0.232

Four hypothesis were stated in the paper:

- **H1 was proved – Authentication methods differ from each other in their usability.** Although usability tests showed that mobile ID was considered the most usable authentication method, ID card and PIN calculator did not trail far behind and were rated highly usable. The Password card was the least usable and scored the lowest in every attribute measured.
- **H2 was proved – Authentication methods differ from each other in their security**. ID card is by far the most secure. The PIN calculator and mobile ID do not differ much in their security. The Password card, the least secure authentication method of the methods researched, is 6 times less secure than an ID card.

- **H3 was disproved - Authentication methods that score high in usability, score low in security.** ID card that was considered highly usable and scored the highest in security. Mobile ID, which was considered most usable, also scored high in security.
- **H4 was proved - Users evaluate usable security of authentication methods rationally.** Survey results showed that ID card is the most usable from 2F authentication methods. Mobile ID was also very highly ranked. This aligned very well with the usability test results. Survey also showed that users believed ID card to be the most secure, and this indeed was proven in the analysis.

Various research has previously suggested that authentication methods cannot be both usable and secure at the same time. The present paper has proven that it is indeed possible for an authentication method to be both usable and secure. A key example is ID cards, which scored best in both usability and security.

Even though 2F authentication methods were ranked a bit lower in usability than authentication via social networks in the survey, they did not rank significantly lower. It also became clear that usability depends on many factors and those factors, in turn, depend on many other factors. It was proven that usability is contextual. 2F authentication methods are widely used in Estonia and it can be possible that using 2F authentication has become a routine for the users, which then makes authentication with 2F more usable. It is important to expand the research on usability of 2F authentication methods further, to see how much the habitual context influences usability.

The present paper evaluated the security of authentication methods with attack trees. However, attack trees as a method has certain shortcomings. When risk needs to be calculated, the probability of the attack needs to be known. It is very difficult to evaluate probabilities without extensive research, and getting probabilities from outside research may not fit into the context of Estonia very well. For example, the probability of insider attack is much lower in Estonia than it is in a bigger country, because the small size of the society restricts this kind of behavior. Further work needs to be done in evaluating probabilities for potential attacks.

References

[1] Aloul, F., Zahidi, S., El-Hajj, W. Two Factor Authentication Using Mobile Phones. – *Proceedings of the IEEE International Conference on Computer Systems and Applications,* 2009, 641-644. [Online] IEEE Xplore (09.08.2015)

[2] Analyzing Likert Scale/Type Data. [WWW] https://www.st-andrews.ac.uk/media/capod/students/mathsupport/Liker.pdf (23.09.2015)

[3] Bagnato, A., Kordy, B., Meland, P.H., Schweitzer, P. Attribute Decoration of Attack-Defence Trees. - *Journal of Secure Software Engineering*. 2012, 3 (2), 1-35. [Online] ACM (09.08.2015)

[4] Braz, C., Seffah, A., M'Raihi, D. Designing a Trade-Off Between Usability and Security: A Metrics Based-Model. – *Human-Computer Interaction, INTERACT 2007: 11th IFIP TC 13 International Conference, Rio de Janeriro, Brazil, September 10-14, 2007: Proceedings. - Lecture notes in Computer Science,* 4663, 114–126. [Online] SpringerLink.LNCS (09.08.2015)

[5] Brostoff. S. Evaluating the usability and security of a graphical one-time PIN system. - *BSC '10 Proceedings of the 24th BCS Interaction Specialist Group Conference, Swinton, UK,* 2010, 88-97. [Online] IEEE Xplore (11.08.2015)

[6] Buldas, A., Laud, P., Priisalu, J., Saarepera, M., Willemson, J. Rational Choice of Security Measures via Multi-Parameter Attack Trees. - Critical Information Infrastructures Security: First International Workshop, CRITIS 2006, Samos, Greece, August 31- September 1, 2006: Proceedings. – Lecture Notes in Computer Science, 2006, 4347, 235–248. [Online] SpringerLink.LNCS (09.08.2015)

[7] Buldas, A., Mägi, T. Practical Security Analysis of E-Voting Systems. – Advances in Information and Computer Security: Second International Workshop on Security, IWSEC 2007, Nara, Japan, October 29-31, 2007: Proceedings. – Lecture Notes in Computer Science, 2007, 4752, 320-335. [Online] SpringerLink.LNCS (09.08.2015)

[8] Causey, B. How to Conduct an Effective IT Security Risk Assessment. – Information Week, 2013. [WWW] http://www.it.vt.edu/ctssr/risk_assessment/documents/strategy-how-to-conduct-an-effective-it-risk-assessment_2411470.pdf (3.10.2015)

[9] Cranor, L.F., Garfinkel, S. Secure or Usable? – IEEE Security & Privacy, 2004, 16-18. [WWW] https://www.computer.org/csdl/mags/sp/2004/05/j5016.pdf (08.07.2015)

[10] Cybernetica. Krüptograafiliste algoritmide elutsükli uuring. – Riigi Infosüsteemi Amet, 2015. [WWW] https://www.ria.ee/public/RIA/Kruptograafiliste_algoritmide_uuring_2015.pdf (15.11.2015)

[11] Cybernetica. Krüptograafilise algoritmide kasutusvaldkondade ja elutsükli uuring. – Riigi Infosüsteemi Amet, 2013. [WWW] https://www.ria.ee/public/PKI/kruptograafiliste_algoritmide_elutsukli_uuring_II.pdf (15.11.2015)

[12] De Cristofaro, E., Du, H., Freudiger, J., Norice, G. A Comparative Usability Study of Two-Factor Authentication. – Cornell University Library, 2014. [WWW] http://arxiv.org/pdf/1309.5344v2.pdf (08.08.2015)

[13] Dimitriadis, C.L. (2007). Analyzing the Security of Internet Banking Authentication Mechanisms. - Information Systems Control Journal 3, 2007. [WWW] http://www.isaca.org/Journal/archives/2007/Volume-3/Pages/Analyzing-the-Security-of-Internet-Banking-Authentication-Mechanisms1.aspx (08.08.2015)

[14] Edge, K.S. A Framework for Analyzing and Mitigating the Vulnerabilities of Complex Systems via Attack and Protection Trees. Air Force Institute of Technology, OH, USA, 2007.

[15] Edge, K., Raines, R., Grimaila, M., Baldwin, R., Bennington, R., Reuter, C. The Use of Attack and Protection Trees to Analyze Security for an Online Banking System. - Proceedings of the 40th Annual Hawaii International Conference on System Sciences, 2007. [WWW] https://www.computer.org/csdl/proceedings/hicss/2007/2755/00/27550144b.pdf (04.10.2015)

[16] e-Estonia. – Estonian Ministry of Foreign Affairs Fact Sheet, 2014. [WWW] http://vm.ee/sites/default/files/elfinder/article_files/e-estonia.pdf (23.09.2015)

[17] Guest, G., Bunce, A., Johnson, L. How Many Interviews Are Enough? An Experiment with Data Saturation and Variability. – Field Methods, 2006, 18 (1), 59-82.

[18] Hiltgen, A., Kramp, T., Weigold, T. Secure Internet Banking Authentication. - IEEE Security and Privacy, 2006, 4 (2), 21-29. [Online] ACM (11.08.2015)

[19] Honan, B. White Paper: Visual Data Security. – Visual Data Security, 2012. [WWW] http://www.visualdatasecurity.eu/wp-content/uploads/2012/07/Visual-Data-Security-White-Paper.pdf (10.10.2015)

[20] How to use Likert scale in Statistical analysis. – Statistics Café, 2011. [WWW] http://statisticscafe.blogspot.com.ee/2011/05/how-to-use-likert-scale-in-statistical.html (23.09.2015)

[21] Information Security course webpage of Institute of Computer Science of University of Tartu. [WWW] https://courses.cs.ut.ee/2013/infoturve/fall/Main/Autentimine (27.09.2015)

[22] Ingoldsby, T.R. Attack Tree-based Threat Risk Analysis. – Amenanza Technologies Limited, 2013. [WWW] https://www.amenaza.com/downloads/docs/AttackTreeThreatRiskAnalysis.pdf (13.11.2015)

[23] Ingoldsby, T.R. Understanding Risk through Attack Tree Analysis. – CSI Computer Security Journal, 2004, 20 (2), 33-59. [WWW] https://www.amenaza.com/downloads/docs/Methodology.pdf (13.11.2015)

[24] Jeffries, R., Miller, J.R, Wharton, C., Uyeda, K. User Interface Evaluation in the Real World: A Comparison of Four Techniques. – CHI '91 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, New York, 1991, 119-124. [Online] ACM (09.08.2015)

[25] Just, M. Authentication Frequency as an Important Design Factor. – SOUPS 2014 WAY Workshop, 2014. [WWW] http://cups.cs.cmu.edu/soups/2014/workshops/papers/frequency_just_15.pdf (08.07.2015)

[26] Jürgenson, A., Willemson, J. Computing Exact Outcomes of Multi-parameter Attack Trees. – On the Move to Meaningful Internet Systems: OTM 2008: Confederated International Conferences, CoopIS, DOA, GADA, IS, and ODBASE 200, Monterrey, Mexico, November 9-14, 2008: Proceedings. – Lecture Notes in Computer Science, 5332, 1036-1051. [Online] SpringerLink.LNCS (09.08.2015)

[27] Jürgenson, A., Willemson, J. (2007). Processing Multi-parameter Attacktrees with Estimated Parameter Values. – Advances in Information and Computer Security: Second International Workshop on Security, IWSEC 2007, Nara, Japan, October 29-31, 2007: Proceedings. - Lecture Notes in Computer Science, 4752, 308-319. [Online] SpringerLink.LNCS (09.08.2015)

[28] Kainda R., Flechais, I., Roscoe, A.W. Security and Usability: Analysis and Evaluation. – Department of Computer Science, University of Oxford, 2009. [WWW] https://www.cs.ox.ac.uk/files/2859/ares_main.pdf (08.07.2015)

[29] Lewis, JR. Sample sizes for Usability studies: Additional considerations. - Human Factors: The Journal of the Human Factors and Ergonomics Society, 1994, 36 (2), 368-378.

[30] Macefield, R. How to Specify the Participant Group Size for Usability Studies: A Practitioner's Guide. - Journal of Usability Studies. 2009, 5 (1), 34-45. [Online] ACM (09.08.2015)

[31] Malicious Insider Threats Greater than Most IT Executives Think. – Computer Economics, 2010. [WWW] http://www.computereconomics.com/article.cfm?id=1537 (15.11.2015)

[32] Maniscalchi, J. Threat vs Vulnerability vs Risk. - Digital Threat, 2009. [WWW] http://www.digitalthreat.net/2009/06/threat-vs-vulnerability-vs-risk/ (13.11.2015)

[33] Murphy, A. Estonia's Mobile-ID: Driving Today's e-services Economy. [WWW] http://www.gsma.com/personaldata/wp-content/uploads/2013/07/GSMA-Mobile-Identity_Estonia_Case_Study_June-2013.pdf (27.09.2015)

[34] Nielsen, J. How Many Test Users in a Usability Study? – Nielsen Norman Group, 2012. [WWW] http://www.nngroup.com/articles/how-many-test-users/ (23.09.2015)

[35] O'Gorman, L. Comparing Passwords, Tokens, and Biometrics for User Authentication. - Proceedings of the IEEE, 2003, 91 (12), 2021-2040. [Online] IEEE Xplore (09.08.2015)

[36] OWASP Risk Rating Methodology. [WWW] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology (23.11.2015)

[37] Reducing Mobile Phone Theft and Improving Security. – Home Office, 2014. [WWW] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/390901/HO_Mobile_theft_paper_Dec_14_WEB.PDF (24.11.2015)

[38] Renaud, K. Evaluating Authentication Mechanisms. - *Security and Usability: Designing secure systems that people can use*. Sebastopol, US : O'Reilly, 2005, 103-128.

[39] Renaud, K. Quantifying the Quality of Web Authentication Mechanisms: A Usability Perspective. – Journal of Web Engineering, 2004, 3 (2), 95-123. [Online] ACM (27.07.2015)

[40] Salter, C., Saydjar, O.S., Schneier, B., Wallner, J. Toward a secure system engineering methodology. – New Security Paradigms Workshop, 1998, 2-10. [WWW] https://www.schneier.com/cryptography/paperfiles/paper-secure-methodology.pdf (24.11.2015)

[41] Sasse, MA., Flechais, I. Usable Security: Why Do We Need It? How Do We Get It? - *Security and Usability: Designing secure systems that people can use*. Sebastopol, US : O'Reilly, 2005, 13-30.

[42] Schneier, B. Attack Trees. – Schneier on Security, 2009. [WWW] https://www.schneier.com/cryptography/archives/1999/12/attack_trees.html (24.11.2015)

[43] Schweitzer, P. Attack-Defence Trees. University of Luxembourg, Luxembourg, 2013.

[44] State Portal eesti.ee. [WWW] https://www.ria.ee/en/government-portal.html (17.10.2015)

[45] Stoneburner, G., Goguen, A., Feringa, A. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. – National Institute of Standards and Technology, Special Publication 800-30, 2002. [WWW] http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (23.09.2015)

[46] The State Portal eesti.ee in numbers. – Riigi Infosüstemi Amet, 2014. [WWW] https://www.eesti.ee/eng/topics/business/riigiportaali_abi/partnerile_1/portal_in_numbers (07.09.2015)

[47] UcedaVelez, T., Morana, M. Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. Hoboken : John Wiley & Sons, Inc, 2015.

[48] Usability Sample Size Calculator. [WWW] http://blinkux.com/usability-sample-size/ (23.09.2015)

[49] Weise, E. 43% of companies had a data breach in the past year. – USA Today, 2014. [WWW] http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/l (13.11.2015)

[50] Weir, CS., Douglas, G., Carruthers, M., Jack, M. User perceptions of security, convenience and usability for ebanking authentication tokens. - Computers & Security, 2009, 28 (1-2), 47-62.

[51] What are brainwaves? [WWW] http://www.brainworksneurotherapy.com/what-are-brainwaves (23.09.2015)

[52] W3C usability page. [WWW] http://www.w3.org/2002/Talks/0104-usabilityprocess/slide3-0.html (02.08.2015)

[53] Yao M., Feng, J. 2011. Evaluating Usability of Three Authentication Methods in Web-Based Application. - Software Engineering Research, Management and Applications (SERA), 2011 9th International conference, 2011, 81–88. [Online] IEEE Xplore (09.08.2015)

[54] Yee, K. User Interaction Design for Secure Systems. – ICICS ’02 Proceedings of the 4th International Conference on Information and Communications Security, London, 2002, 278-290. [Online] ACM (09.08.2015)

[55] 5 types of Brain Waves Frequencies: Gamma, Beta, Alpha, Theta, Delta. [WWW] http://mentalhealthdaily.com/2014/04/15/5-types-of-brain-waves-frequencies-gamma-beta-alpha-theta-delta/ (23.09.2015)

Appendix 1 – Detailed survey answers

Table 14. Responses to survey question „How do you rate the usability of each authentication method".

Answer Options	**Very complicated to use**						**Very easy to use**	**Rating average**	**Response count**
Social Networks	15	13	19	26	21	53	177	5.75	324
ID card	11	21	23	43	47	67	167	5.54	379
Mobile ID	15	20	15	32	33	44	146	5.50	305
Bank password card	10	21	17	66	44	62	147	5.42	367
PIN calculator	13	21	23	42	58	69	137	5.39	363

Table 15. Responses to survey question „How do you rate the security of each authentication method".

Answer Options	**Very complicated to use**						**Very easy to use**	**Rating average**	**Response count**
Social Networks	148	87	50	41	16	11	3	2.26	356
ID card	3	1	3	12	26	128	206	6.34	379
Mobile ID	6	10	11	38	36	85	133	5.74	319
Bank password card	5	4	16	37	78	108	118	5.66	366
PIN calculator	2	8	17	37	33	101	110	5.71	314

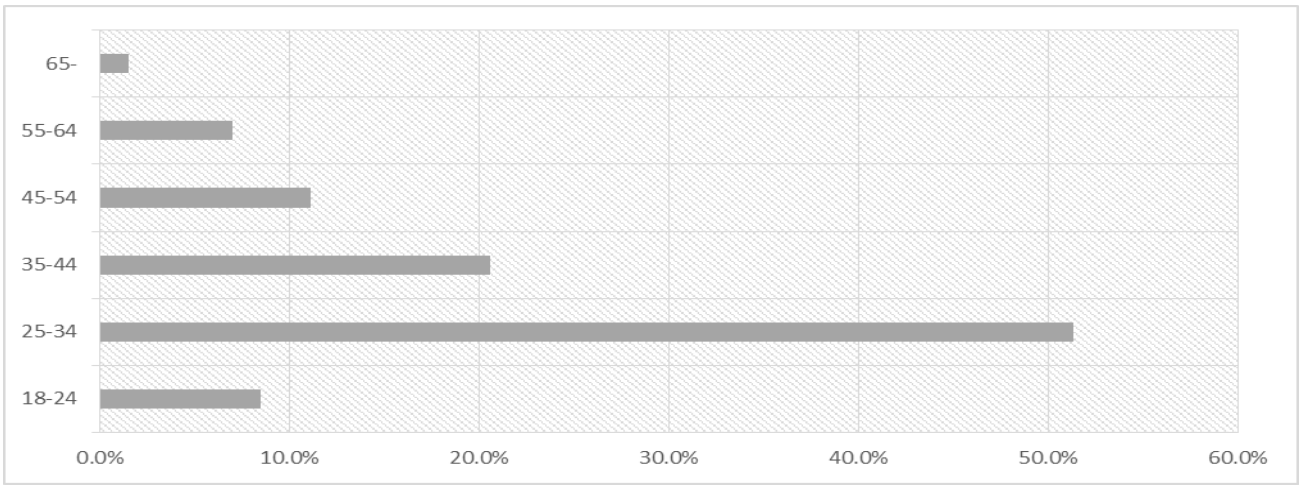

Figure 9. Survey participants by age.

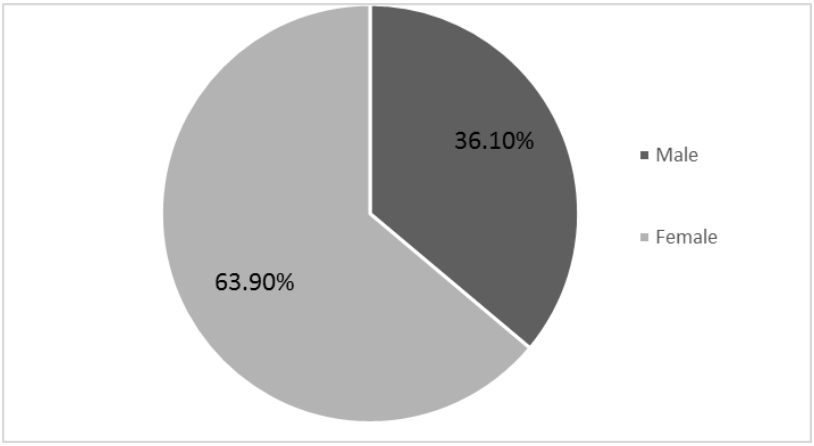

Figure 10. Survey participants by gender.

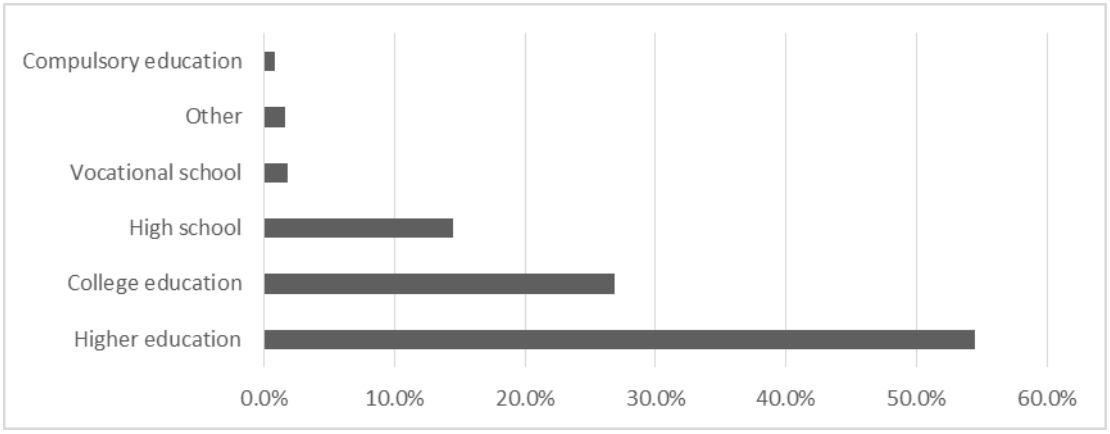

Figure 11. Survey participants by education level.

Appendix 2 – Number of authentication steps

- ID card: 6
    1. Insert ID card to a reader
    2. Click on “Enter”
    3. Click on “login with ID card”
    4. Select a certificate to use
    5. Enter PIN1
    6. Click on “OK”
- Mobile ID: 5
    1. Click on “Enter”
    2. Type in a personal code
    3. Type in a mobile phone number
    4. Enter PIN1 on mobile phone
    5. Click on “OK” on mobile phone
- PIN calculator: 9
    1. Click on “Enter”
    2. Click on a specific bank
    3. Enter username/user number
    4. Activate PIN calculator
    5. Enter PIN to a calculator
    6. Choose a programme number on a PIN calculator
    7. Enter password from the calculator to the interface
    8. Click on “OK”
    9. Click on a message “Sending information to the service provider”
- Password card: 8
    1. Click on “Enter”
    2. Click on a specific bank
    3. Enter username/user number
    4. Enter a password
    5. Click on “OK”
    6. Enter a needed password from the password card
    7. Click on “OK”
    8. Click on a message “Sending information to the service provider”

Appendix 3 – Detailed usability answers

Table 16. Detailed usability test answers of ID card and mobile ID.

Convenient to use	Speed of using device	Degree of enjoyment	Would use device again	User-friend-liness	Trust-worth-ness	Easy to use without instructions	Didn't demand high concen-tration	Stress free	Didn't cause frustration	Not complicated	Degree of security	Easy to use for the first time	Time	Method	Gender
6	6	6	6	5	6	6	5	4	6	6	6	5	44.35	ID card	W
6	6	6	6	5	6	6	5	6	6	5	6	6	41.07	ID card	M
4	5	5	6	5	6	5	2	6	5	4	6	3	83.27	ID card	W
6	6	6	6	6	6	1	1	6	6	6	6	6	118.19	ID card	W
6	6	5	5	5	6	3	4	6	6	5	5	4	32.06	ID card	M
5	5	4	6	5	5	6	6	6	6	6	5	5	51.22	ID card	W
6	6	6	4	6	6	6	6	6	6	6	5	5	35.57	ID card	W
6	6	6	6	6	6	6	5	6	6	6	6	6	33.92	ID card	M
6	6	4	6	6	4	5	5	6	6	6	4	5	49.33	ID card	M
3	4	5	5	6	5	6	5	6	5	5	5	5	83.27	ID card	W
6	5	6	4	6	6	5	6	6	6	6	6	5	46.76	Mobile ID	W
4	3	3	4	5	5	2	5	5	4	4	5	4	82.09	Mobile ID	M
5	5	4	5	5	6	4	6	6	6	5	4	5	59.37	Mobile ID	W
6	6	6	6	6	6	6	6	6	6	6	6	3	80.16	Mobile ID	W
6	6	6	6	6	6	6	6	6	6	6	6	6	53.31	Mobile ID	M
6	6	6	6	6	6	6	6	6	6	6	6	6	62.11	Mobile ID	W
6	6	6	6	5	6	4	6	6	6	6	6	5	48.92	Mobile ID	W
6	6	6	6	6	6	6	6	6	6	6	6	6	53.28	Mobile ID	M
5	5	6	5	6	6	5	5	5	5	5	5	4	111.95	Mobile ID	M
6	6	6	6	6	6	4	6	6	6	6	6	4	51.54	Mobile ID	W

Table 17.. Detailed usability test answers of password card and PIN calculator.

Convenient to use	Speed of using device	Degree of enjoyment	Would use device again	User-friend-liness	Trust-worth-ness	Easy to use without instructions	Didn't demand high concen-tration	Stress free	Didn't cause frustration	Not complicated	Degree of security	Easy to use for the first time	Time	Method	Gender
6	6	6	6	6	6	1	5	6	6	6	6	6	91.9	Password card	M
6	6	6	6	6	6	4	6	6	6	6	6	6	137.15	Password card	W
6	6	5	5	6	5	2	4	6	6	6	6	6	48.05	Password card	M
5	5	6	5	5	5	2	2	5	5	3	5	5	79.98	Password card	W
6	1	3	3	4	4	6	1	1	1	2	5	3	66.56	Password card	W
6	6	4	6	5	4	6	4	3	5	6	3	6	66.84	Password card	W
6	6	6	6	6	6	6	6	6	6	6	2	6	48.84	Password card	M
3	2	1	1	4	6	6	2	5	6	6	6	5	53.19	Password card	W
4	4	5	6	1	5	6	3	5	6	3	6	5	49.22	Password card	M
5	6	6	6	6	6	5	5	6	6	6	5	6	117.35	Password card	W
5	4	4	3	5	6	6	5	5	6	6	6	5	48.6	PIN calculator	W
5	4	4	5	5	6	2	5	5	6	6	5	5	95.09	PIN calculator	M
5	5	4	6	5	5	6	5	5	6	5	5	6	54.99	PIN calculator	W
6	5	6	6	5	6	6	6	6	6	6	5	5	60.24	PIN calculator	W
5	6	6	4	6	5	6	4	6	6	6	5	6	56.3	PIN calculator	M
6	6	6	6	6	4	6	6	6	6	6	4	5	51.53	PIN calculator	W
5	5	6	6	5	3	5	5	5	5	5	5	3	58.27	PIN calculator	M
5	4	5	5	6	5	6	6	5	6	5	5	3	156.37	PIN calculator	M
5	5	4	6	6	5	6	5	6	4	6	5	6	44.66	PIN calculator	W
6	5	6	5	4	5	6	6	6	6	6	6	6	42.97	PIN calculator	M