



Aalto-yliopisto

Aalto University

Joonas Kurikka

---

# Balancing usability and security in the business cloud authentication

---

Master's Thesis

Espoo, 27th May 2013

Supervisor Marko Nieminen

Instructor Massimo Nardone

AALTO UNIVERSITY SCHOOL OF ELECTRICAL ENGINEERING	ABSTRACT OF THE MASTER'S THESIS	
Author: Joonas Kurikka		
Title: Balancing usability and security in the business cloud authentication		
Department of Communications and Networking		
Professorship: Cognitive technology	Code: S-114	
Supervisor: Prof. Marko Nieminen		
Instructor(s): M.Sc (Tech) Massimo Nardone		
<p>Increasing wave of cloud services is creating many new ways for remote workers, outsourcing partners and hackers to access the essential tools and business data of the cloud-enabled companies. As the amount of business critical data in the cloud services increase, so does the need for securing it. Securing a cloud service needs balanced defenses against many different attack vectors in various levels of the service, starting from the edges of the public network and continuing deep inside the individual design of the each software component of the cloud service.</p> <p>One of the biggest attack vectors is also the one route that has to be left open for the legitimate users to use the service – user authentication. The goal for this thesis was to find balance between making the user authentication in business cloud services secure enough and usable enough. Authentication has to be secure enough to prevent malicious attackers from gaining access to the valuable data and resources inside the service. At the same time it has still to be usable enough for the legitimate users to be able to access their cloud services without unnecessary frustration.</p> <p>The topic is approached through literature review of relevant research and relevant authentication methods. In addition, several (n=6) usability tests are performed in combination with half-structured interviews to evaluate the user preference in authentication method selection and the factors affecting the experienced balance of security and usability. In addition, the thesis evaluates other important factors, in addition to the authentication method itself, that are affecting the security – usability –balance of the entire authentication process.</p> <p>As a result the thesis presents several ways to improve the balance of usability and security in business cloud services. Multifactor authentication is observed to be more usable than equally secure single-factor authentication. Educating the users and communicating the security needs clearly helps to reduce the unsanctioned security “shortcuts” that reduce the overall security. Authentication resetting is often neglected, but really essential factor both as usability hindrance and possible attack vector.</p>		
Date: 27.05.2013	Language: English	Number of pages: 89 + 10
Keywords: usability, security, authentication, cloud computing, virtualization		

AALTO-YLIOPISTO SÄHKÖTEKNIIKAN KORKEAKOULU		DIPLOMITYÖN TIIVISTELMÄ	
Tekijä: Joona Kurikka			
Työn nimi: Balancing usability and security in the business cloud authentication			
Tietoliikenne- ja tietoverkkotekniikan laitos			
Professori: Kognitiivinen teknologia		Koodi: S-114	
Työn valvoja: Prof. Marko Nieminen			
Työn ohjaaja(t): M.Sc (Tech) Massimo Nardone			
<p>Jatkuvasti suosiotaan kasvattavat pilvipalvelut luovat monia uusia mahdollisuuksia etätyöntekijöille, yhteistyökumppaneille ja hakkereille päästä käyttämään yrityksen työkaluja ja asiakastietoja. Kun pilvipalveluissa olevan tärkeän yritysdatan määrä kasvaa, myös palveluiden tietoturva-vaatimukset kovenevat. Pilvipalveluiden tietoturvalisessä suunnittelussa tulee ottaa huomioon lukuisia erilaisia hyökkäysreittejä monella eri palvelun tasolla aina verkon rajapinnasta yksittäisten ohjelmistokomponenttien haavoittuvuuksiin.</p> <p>Yksi isoimmista hyökkäysvektoreista on myös reitti, joka on pakko jättää osittain avoimeksi palvelun varsinaisia käyttäjiä varten – autentikointi, eli käyttäjien todentaminen palveluun kirjautumisen yhteydessä. Diplomityön tavoitteena oli löytää tasapainokohta ja siihen vaikuttavat tekijät pilvipalveluiden käytettävyyden ja tietoturvan väliltä. Käyttäjän autentikoinnin tulee olla tarpeeksi tietoturvallinen, etteivät mahdolliset hyökkääjät pääsisi käsiksi järjestelmän arvokkaisiin dataan ja resursseihin. Samaan aikaan autentikoinnin tulee olla myös tarpeeksi käytettävää, jotta varsinaiset käyttäjät pääsevät palveluihinsa tehokkaasti ja ilman tarpeetonta turhautumista.</p> <p>Aihetta lähestytään kirjallisuuskatsauksella aihealueen keskeiseen tutkimukseen ja pilvipalveluihin sopivien autentikointimenetelmien kartoittamisella. Näiden lisäksi työssä suunniteltiin ja järjestettiin kuudelle osallistujalle käytettävyydesti, jossa mitattiin käyttäjien suhtautumista neljään erilaiseen autentikointimenetelmään ja niitä yhdistelevään monen menetelmän autentikointiin (multi-factor authentication). Samalla käyttäjiltä kartoitettiin puolistrukturoiduilla haastatteluilla erilaisia tekijöitä, jotka vaikuttavat heidän kokemaansa käytettävyyden ja tietoturvan tasapainoon.</p> <p>Tutkimuksessa tunnistettiin useita tapoja parantaa käytettävyyden ja tietoturvan tasapainoa yritysten pilvipalveluissa. Monen keskivahvan autentikointimenetelmän yhdistelmän havaittiin olevan käyttäjäystävällisempi kuin samaan tietoturvan tasoon yltävän yhden menetelmän vahvan autentikaation. Käyttäjien kouluttamisella ja tietoturvan tavoitteiden selkeällä kommunikaatiolla oli myös iso merkitys, etenkin epävirallisten, tietoturvaa heikentävien ”kiertoteiden” välttämässä. Unohtuneiden käyttäjätunnusten uudelleenasettaminen on myös eräs usein liian vähälle huomiolle jäävä tekijä, jolla on iso vaikutus sekä järjestelmän käytettävyyteen että tietoturvaan.</p>			
Päivämäärä: 27.05.2013		Kieli: Englanti	Sivumäärä: 89 + 10
Avainsanat: käytettävyys, tietoturva, kirjautuminen, pilvipalvelut, virtualisointi, autentikointi			

# Acknowledgements

---

I want to thank my supervisor Marko Nieminen for all the feedback and guidance I have received and IBM Finland for providing me with the resources and experience that this thesis was built on. I would also like to thank Hanna Poranen for her help with the thesis layout.

Finally, I would like to thank my family and friends, especially the friends and test subjects at ME310 for all the support and encouragement I have received during the whole thesis process.

---

---

Joona Kurikka

Helsinki, 27.5.2013

# Table of Contents

Tiivistelmä	ii
Abstract	iii
Acknowledgements	iv
Table of Contents	v
Abbreviations	viii
1 Introduction	1
1.1 Scope	3
1.2 Objective	3
1.3 Structure of the thesis	4
2 Background	5
2.1 The Cloud	6
2.1.1 Service models	6
2.1.2 Deployment models	8
2.1.3 Desktop as a Service - Desktop Cloud	10
2.2 Usability	11
2.2.1 Usability according to Nielsen	11
2.2.2 Usability according to ISO 9241-11	14
2.3 Security	16
2.3.1 Internal security	18
2.3.2 External security	20
3 Balancing Usability and Security	22
3.1 Passwords	23
3.2 Stealing passwords	25
3.3 Communicating with the user	25
3.4 Punishing the users who break the rules	26
3.5 The weakest link?	27
4 Authentication methods and situations	28
4.1 Something you know	29
4.1.1 User ID and password	30
4.1.2 PwdHash – Service-specific passwords through hashing	30

4.2	Something you have	31
4.2.1	RSA SecurID – hardware token	31
4.2.2	Software token	32
4.2.3	SMS token	32
4.2.4	Email token	33
4.3	Something you are	33
4.3.1	Fingerprints	34
4.3.2	Face recognition	34
4.3.3	Iris scanners	34
4.3.4	Voice recognition	35
4.4	Somebody you know	35
4.5	Sharing	35
4.5.1	Corporate systems	36
4.5.2	Online APIs	36
4.5.3	TUPAS in Finland	36
5	Empirical study	37
5.1	Purpose and scope definition	38
5.2	Context and roles definition	39
5.3	User selection	41
5.4	Task definition	41
5.5	Measurement apparatus design	42
5.6	Technical setup	44
5.7	Technical setup alternatives	46
5.7.1	Deciding the platform	46
5.7.2	Deciding the software components	47
6	Results	50
6.1	Demographics	51
6.2	Usability – Efficiency	54
6.3	Usability – Effectiveness	55
6.4	Usability – Satisfaction	56
6.5	Comparative rating	58
6.6	User insights	60
6.6.1	SMS OTP	60
6.6.2	Email OTP	61
6.6.3	Pledge client	62
6.6.4	Strong authentication overall	63
7	Conclusions and discussion	64
7.1	Answering the research questions	65
7.2	Validity and credibility of the study	68
7.3	Implementing the results in practice when designing business cloud authentication	69
7.4	Ideas for future research	70

References	71
Appendices	78
Appendix A: Usability of security in Likert scale	79
Appendix B: Participant comments from the debriefing interview	80
Appendix C: Pre-questionnaire for the test participants	84
Appendix D: Likert questionnaire for the test participants	88

# Abbreviations

<b>AaaS</b>	Architecture as a Service
<b>AD</b>	Active Directory
<b>API</b>	Application programming interface
<b>BaaS</b>	Business as a Service
<b>CaaS</b>	Computing as a Service
<b>CRM</b>	Customer relationship management
<b>CRMaas</b>	CRM as a Service
<b>CSS</b>	Cascading Style Sheets
<b>DaaS</b>	Desktop as a Service
<b>DBaaS</b>	Database as a Service
<b>EaaS</b>	Ethernet as a Service
<b>FaaS</b>	Frameworks as a Service
<b>FAR</b>	False Acceptance Rate
<b>FRR</b>	False Rejection Rate
<b>GaaS</b>	Globalization or Governance as a Service
<b>HaaS</b>	Hardware as a Service
<b>IBM</b>	International Business Machines
<b>IMaaS</b>	Information as a Service
<b>IaaS</b>	Infrastructure or Integration as a Service
<b>IDaaS</b>	Identity as a Service
<b>LaaS</b>	Lending as a Service
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>MaaS</b>	Mash-ups as a Service
<b>MSISDN</b>	Mobile Subscriber Integrated Services Digital Network-Number
<b>OaaS</b>	Organization or Operations as a Service
<b>OTP</b>	One Time Password
<b>RQ</b>	Research question
<b>SaaS</b>	Software or Storage as a Service
<b>SCE</b>	SmartCloud Enterprice
<b>SMS</b>	Short Message Service
<b>PaaS</b>	Platform as a Service
<b>TaaS</b>	Technology or Testing as a Service
<b>VaaS</b>	Voice as a Service
<b>VPN</b>	Virtual Private Network
<b>XaaS</b>	Everything as a Service



# 1 Introduction



The nature of knowledge work is changing and workers spend less and less time on their dedicated workstations at the office. Some companies do not even have the traditional office facilities anymore, and the “office” is divided in private homes around four continents (Brebaugh et al., 2012).

During the last decade the internet connection speeds have increased and the cost of computational speed has decreased. This has allowed a set of new alternatives to gain popularity among the mobile workers and their employees. These centralized remote working solutions are usually categorized under the term Cloud Computing or Business Cloud (Pallis, 2010). As Pallis (2010) describes, cloud computing itself is a wide, multidisciplinary field that is considered to be a convergence of several independent computing trends, such as Internet delivery, “pay-as-you go” utility computing, elasticity, virtualization, grid computing, distributed computing, storage, content outsourcing, security, and Web 2.0.

There are an extensive amount of different kinds of cloud computing offerings already on the market, and the field is growing fast. At the moment there is one constant definition of cloud computing. According to the common definition (NIST, 2011), the shared denominator of all the cloud services is that the data is located at remote servers and users can access it from almost anywhere over the internet with any suitable device.

One of the latest Cloud Computing offering to gain popularity in the business world is the Desktop Cloud, also known as Desktop-as-a-Service (DaaS). The Desktop Cloud solutions create a virtual desktop, which contains all the necessary desktop programs and access to the corporate data. The workers can then access their new personal desktop remotely with any computer they have at hand. (Beaty et al., 2009)

There is a huge potential for more efficient use of resources and a need for fast scaling as the business realities change. Desktop Cloud solutions can help companies to create savings on the heavy local desktop and server infrastructure. They can also provide the end users a lot more work satisfaction by allowing them to follow their preferences on the endpoint devices with strategies like “bring your own device” (BYOD) (Burt, 2011). The cloud services also make it easier to hire temporary workers and find suitable workers anywhere, as the virtual desktops can be re-provisioned to users without any physical delays and accessed over the public internet from all around the world in minutes after the creation.

However, these ubiquitous access alternatives have also a negative side in the form of security risks. When the ICT infrastructure of the company is opened for employees to have the necessary access to use the cloud services, the same openings can be used for malicious purposes. Some of the companies are completely avoiding the cloud services because of these security risks. But as the cloud evolves and offers increasingly appealing alternative to the “traditional” offline computing. Even the late adopters are starting to look into the Cloud and to the different security system alternatives to minimize the risks. (Market-Visio, 2013)

## 1.1 Scope

There are various alternative methods to improve the security in the cloud services, starting from the outermost layer, located right next to the public network and continuing deep inside the services. For this thesis the scope will be limited to the first line of defense that all the services have in common – access control and user authentication. This thesis will take a deeper look in to various authentication techniques and how they should be implemented in the business cloud computing environment.

This thesis will take a closer look at one of the fastest growing areas of the business cloud offering, Desktop-as-a-Service –solutions (DaaS), and especially the authentication methods used. As almost all of the affiliated companies are using DaaS solutions for critical software and data access alternatives, the business DaaS solutions are one of the most security-critical areas of the overall cloud services. The Desktop side of the business cloud is also the most interesting focus for Integrated Technology Services (ITS) department at IBM Finland, which is sponsoring this thesis.

## 1.2 Objective

This thesis was conducted with IBM Finland to provide insights and new implementation ideas for authentication solutions in business cloud environments. The author has been working for IBM Finland for two years, designing and implementing DaaS environments and other business cloud solutions. The thesis started as a project to support implementing even more usable and secure authentication solutions to customer environments. The authentication phase was observed to be one of the critical elements for the customers when selecting a service provider, thus even small improvements to the current solutions could have a big impact in the tough competition.

The assumption for the research in this thesis is that the levels of usability and security of the authentication methods have a negative correlation (Whitten et al., 1999). In the most extreme cases the system is 100% secure, and as a result even the intended users are unable to access it. On the opposite extreme all the users, even the unintended ones, can access the cloud services without any hindrances from the security systems, making the system totally unsecure. All of the examples in the real world are assumed to rest somewhere between these two extremes.

This thesis aims to define an implementable authentication strategy that meets or exceeds the usability expectations of typical business users. At the same time the authentication strategy should meet the complex security demand of the business context. This aim is approached with three research questions:

**Rq1** Identify a) the common authentication methods used in business cloud authentication at the moment and b) emerging new authentication methods suitable for the purpose.

**Rq2** What are the most important factors, in addition to the authentication method itself, that are affecting the security – usability –balance of the whole authentication process and how they can be optimized for the business cloud authentication?

**Rq3** How the usability and security aspects of authentication methods affect the user preference in method selection?

These research questions are answered with a combination of a literature review and an empirical study.

## 1.3 Structure of the thesis

This thesis will include a literature review and an empirical study. Chapter two presents the background info of the key concepts used in this thesis: cloud computing, usability and security.

Chapter three will extend these key concepts and their relations to each other. The chapter will also cover some of the recent cloud security related events that have had an impact to the industry development.

Chapter four will introduce the three traditional categories of authentication methods and their more recent extensions. Several examples of authentication methods from each category have also been selected for a closer introduction. The introduced methods were selected based on their estimated relevance on the business cloud authentication context.

Chapter five will present the construction of the empirical study and the theoretical and technical backgrounds for it. The results of the study will then be presented and analyzed in chapter six.

Chapter seven presents the condensed answers for the research questions and recommendations for cloud service authentication planning. Chapter seven will also conclude the thesis and present ideas for the future research.

## 2 Background



This chapter will present the essential background info for this thesis. The definition of cloud services will be discussed from the perspective of service- and deployment models, and we'll take a closer look into service model known as Desktop as a Service, which will be the case example in this thesis. The chapter will also present the detailed definitions of overall Usability and Security.

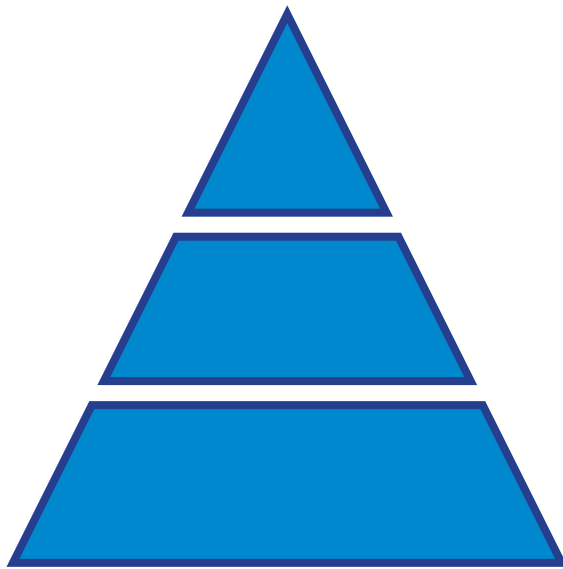
## 2.1 The Cloud

### 2.1.1 Service models

The terms “Cloud” or “Cloud Computing” entered the public discussion around year 2000, and The terms “Cloud” or “Cloud Computing” entered the public discussion around year 2000, and were at first considered yet another buzzword dictionary for old solutions (Pallis, 2010).. After over a decade of ever increasing popularity of cloud computing (Market-Visio, 2013), the debate around the exact definition of “The Cloud” is still going on. Many reputable authors have given their attempts in defining the concept (Armbrust et al., 2010; Buyya et al, 2009), but nobody has managed to do it undisputedly. When for example the National Institute of Standards and Technology (NIST) published their definition of Cloud Computing in September 2011 (Mell et al., 2011), it got a lot of criticism (McKendrick, 2012; Yung, 2011) for excluding certain borderline concepts.

National Institute of Standards and Technology (NIST, 2011) defines the Cloud Computing to be “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

NIST definition also describes the Cloud to be composed of three distinctive service models, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a service (IaaS), as found below in Figure 1.



**Software as a Service**

**Platform as a Service**

**Infrastructure as a Service**

*Figure 1: The cloud service models*

---

In SaaS service model, the Cloud provides end users the ability to use applications running on a cloud infrastructure via various devices, such as laptops, tablets or even mobile phones. Most of the consumer cloud products like webmail and file storage services are SaaS offerings, and the business model is popular among the business users as well (Marston et al., 2011).

In PaaS offerings the customer is provided with a customizable platform that supports predefined types of applications, libraries, tools and programming languages. In other words, this means that each platform provider has built their platform offerings with distinctive set of applications and supported languages, which might make switching providers a really challenging and expensive task. The customer has full control over the supported solutions, but not for the underlying cloud infrastructure or the amount of supported applications.

IaaS service model is the most flexible of the three in terms of customizability. The customer gets full control over the provisioned resources from the provider's cloud infrastructure and is free to deploy any operating systems or stand-alone applications on them.

In addition to these three most common service models, there is almost unlimited amount of other XaaS (Everything as a Service) offerings, which include services like AaaS (Architecture as a Service), BaaS (Business as a Service), CaaS (Computing as a Service), and so on. As there are no rules or regulations on XaaS acronyms, it is certain that the Cloud industry will supply a steady stream of new aaS'es as the offerings expand to new service models (IBM, 2008). These acronyms are in no way standardized or controlled, which means that there exists a lot of overlapping and inconsistencies in terminology. For example one vendors' VaaS can be called SaaS by another vendor.

To sum it up, the terms "Cloud" and "Cloud Computing" are as elastic and flexible as the services they describe. Due to this elasticity and varying interests of the different actors in the Cloud business, it is likely that a solid definition will never be reached. At least not before "The Cloud" itself gets replaced by the next step in the evolution of the global ICT environment.

## 2.1.2 Deployment models

There are four different deployment models for the cloud services: private, community, public and hybrid. They differ from each other by cost, security level and potential user base. (NIST, 2011)

### Private cloud

The cloud infrastructure is built for a single organization and can include any number of end users that belong to that specific organization. Private clouds can be owned, managed and operated by the organization itself, a third party, or some combination of them.

A private cloud infrastructure is the most secure deployment model for the cloud as no outsiders have legitimate access to the infrastructure, and the organization has full control over the permissions and the authentication process.

On the flipside, private clouds lose a part of the flexibility present in other deployment models, as the resources can be scaled and distributed only inside of a single organization. Depending on the deployed cloud service, the effect of privatization to the cloud cost structure might vary from minimal to very high, compared to shared resources.

In some situations a private cloud might be only possible deployment model due to external reasons e.g. software licenses or security requirements.



## **Community cloud**

The user base of community cloud can consist of end users in several different organizations that belong to the same “community”, e.g. share some interests or requirements relevant to the cloud infrastructure. Community cloud can be managed by any of the companies belonging to the “community” or a third-party service provider.

Community cloud can be regarded as an “extended private cloud”, in which the member companies can control the membership of the community. Each company can also know who they are sharing the infrastructure with, and who are the outsiders having a potential in-cloud access to their systems e.g. through unpatched security holes.

With the community cloud model, participating companies can benefit from the economics of scale by optimizing the cloud hardware with their partially overlapping usage needs. The community cloud is still not as flexible as the huge public clouds, but it is certainly more efficient than using the same applications in separate private clouds.

## **Public cloud**

The public cloud, as the name implies, is open to anyone. The cloud infrastructure is provided by a private service provider or a public organization and anyone can participate as long as they meet the pre-defined access requirements, for example paying the monthly fee.

The entire public cloud infrastructure usually exists in the premises of the cloud provider, and they can scale the infrastructure according to the estimated usage and profiling. For example if the user base is divided in different time zones, the core infrastructure can manage more evenly divided load throughout the day.

In terms of security, public cloud services can cause some concerns for the companies. They do not know who they are sharing the infrastructure with in cases of possible data mix-ups and security breaches. And they do not have any way to monitor the cloud provider, who has the full administrative rights to all of their operations and data in the public cloud.

## **Hybrid cloud**

Hybrid cloud infrastructure is a composition of two or more different cloud deployment models. In a hybrid cloud, different deployment models are separate entities that are bound together by some technology that enables data and application portability between different clouds.

Hybrid clouds can be used, for example, for load balancing DaaS services. If the company’s private cloud cannot handle the peak traffic during a busy time of the year, it can burst the extra virtual desktops to a community cloud which is built for such occasions by a few partner companies with different peak seasons.

### 2.1.3 Desktop as a Service - Desktop Cloud

This thesis will focus on a sub-category of PaaS service model, Desktop as a Service - DaaS. In DaaS, the cloud platform offering is extended to cover all the aspects of everyday computing of the end users. The DaaS offerings usually cover all the interaction interfaces between the end users and the rest of the company infrastructure, all of the things that the traditional company-provided laptop would include. The actual setup of DaaS environments varies a lot depending on the needs of the company, but DaaS offering usually includes access to a pre-defined set of programs and data storages and limited or unlimited access to corporate network resources. Currently all the biggest business DaaS offerings are built with Microsoft Windows. Two of the main reasons for this operating system selection are compatibility with the existing business software and offering the end users a familiar interface to the system. (Beaty et al., 2009)

There are several reasons why companies are implementing or planning to implement DaaS solutions in their environment, but usually the three main factors are control, price and connectivity in varying order of importance. It is possible to use DaaS to achieve a lower TCO (a total cost of ownership) or more efficient end-user solutions than with traditional infrastructure based solely on a local hardware computing. In some cases it might even be possible to achieve both of these goals simultaneously.

The DaaS solutions also create new possibilities to manage the whole business infrastructure. For example a concept called Bring Your Own Device (BYOD) empowers the end users to select their own tools and still be compliant with the company IT processes and requirements (Burt, 2011).

## 2.2 Usability

This section presents the viewpoint to usability from two different perspectives that are approaching the definition from different directions and thus complementing each other. Jacob Nielsen approaches the definition (Nielsen, 1993) with a lot of practical experience from conducted usability testing. Other viewpoint comes from the academic research of the International Organization for Standardization, as the ISO 9241-11 (ISO, 1998) defines context of use and measurements for evaluating usability in set contexts.

### 2.2.1 Usability according to Nielsen

According to the definition of Jacob Nielsen (Nielsen, 1993), usability is a sub-concept of usefulness, together with utility. Utility means that the system can perform all the tasks that it needs to perform and usability is used to define how easy it is for the users to actually perform these actions. Usability is further composed of five factors: learnability, efficiency, memorability, amount of errors and satisfaction.

Usefulness itself is a further sub-category in Nielsen's general definition (Figure 3). The main definition of system-level acceptability is divided in social and practical acceptability. Social acceptability is more about feeling and opinions than technical solutions; how the people in general see the system and do they accept its functions like gathering or publishing data. The practical acceptability in turn consists of the practical measurements of acceptability like cost, reliability and compatibility. Usefulness is in turn a sub-category of practical acceptability.



Figure 2. Breakdown of system acceptability (Nielsen, 1993).

---

## **Learnability**

Learnability can be evaluated by measuring how easy is it for users to accomplish basic tasks the first time they encounter the design. Systems that are aimed for professional users can have a longer learning curve if the intention is to eventually achieve a higher skill level. However, systems intended for novice users or only for occasional use need to be faster to learn to meet the usability requirements.

## **Efficiency**

Efficiency of a system is the level of performance the user can achieve through practice. The efficiency can be measured by measuring the completion time of a task over several recursions. When the additional practice does not affect the performance anymore, the user has reached his maximum efficiency with the system. These measurements can then be used to benchmark the efficiency level of other users.

## **Memorability**

Memorability is about the proficiency of users with a system design, when they use it after a period of inactivity. When users return to the design, how easily can they re-establish proficiency? This can be best measured with a performance testing, as the users can remember the usage practices of a system without remembering specific menu terms or icons.

## **Errors**

There are several levels of errors that the user can encounter in a system. Some of the lower levels of errors do not necessarily require any actions, especially if recovering from them is trivial for the user. On the other hand, especially catastrophic errors that have serious consequences to the ongoing tasks should be analyzed in great detail.

## **Satisfaction**

The subjective satisfaction of use is extremely important and can be in a major role when the user decides about the future use of the system. The satisfaction should be asked only after the actual use of the system, as the correlation between answers before and after the actual use tend to be low (Root et al., 1983).

## 2.2.2 Usability according to ISO 9241-11

The International Organization for Standardization defines usability in ISO 9241-11 as “the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use” (ISO, 1998).

This means that the standard measures usability with achieving the goals from three axes: Effectiveness, Efficiency and Satisfaction.

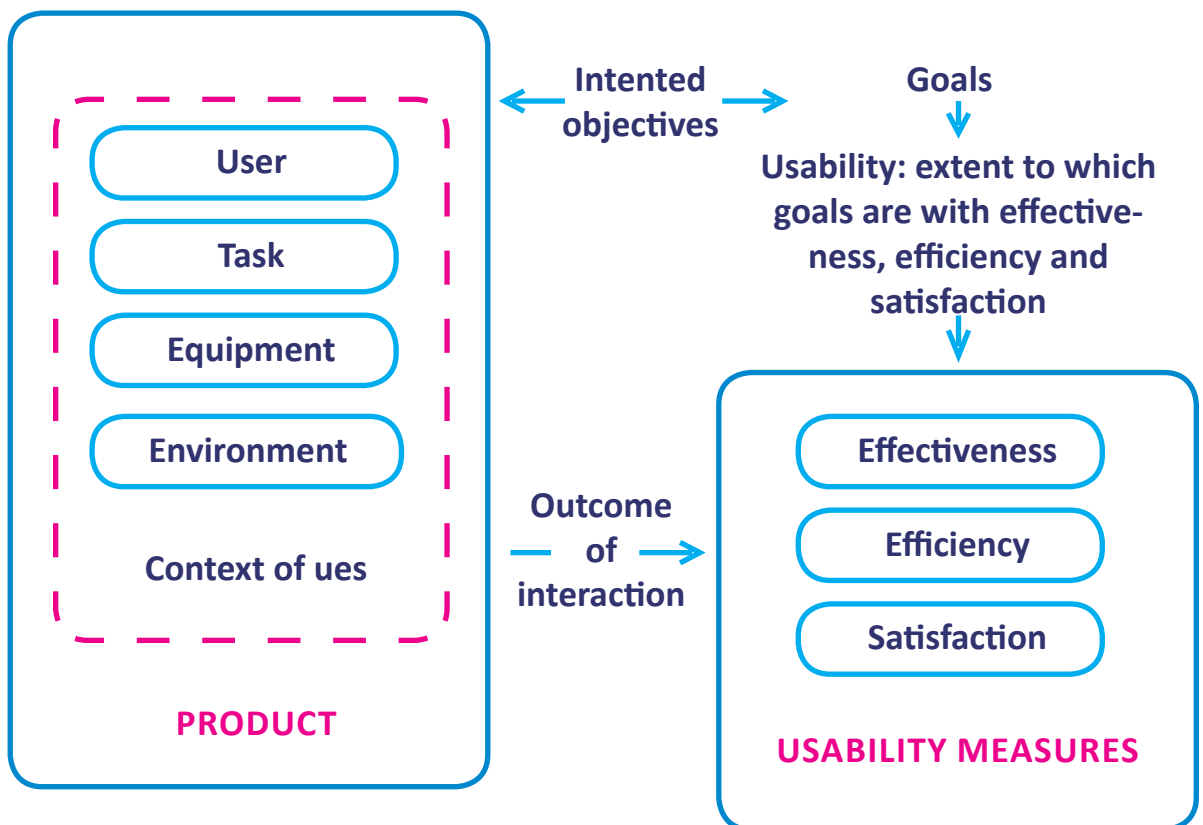


Figure 3. Usability framework (ISO, 1998).

## **Effectiveness**

Effectiveness measures how well do the users achieve their goals using the system, e.g. what percentage of a task can be completed within set boundaries.

## **Efficiency**

Efficiency is the relationship of used resources (e.g. time) to the achieved effectiveness.

## **Satisfaction**

Satisfaction measures how the users feel about their use of the system and what is their rate of voluntary use.

## **User**

Users should be described by clearly defining all their important characteristics (related to the system). The definition should be done on a level of individual users, as the characteristics-level definition does not take into account the different combinations of characteristics inside individual user types.

## **Task**

Tasks are the actions that users need to do in order to reach the goal. The tasks should be always analyzed in the context of the targeted goals. The performed tasks are usually identified by using a task analysis methodology.

## **Equipment**

All the context-related equipment and their properties should be described in detail. As the user interacts with the system through the related equipment, they might have a big impact on the system usability.

## **Environment**

All the relevant attributes of the physical and social environment need to be described. These might include attributes of the wider technical environment (e.g. the local area network), the physical environment (e.g. workplace, furniture), the ambient environment (e.g. temperature, humidity) and the social and cultural environment (e.g. work practices, organizational structure and attitudes).

## **Goals**

The goals and the criteria that satisfy them should be described in detail. The goals can also be described in form of all the sub-goals that are needed to reach to the actual goals. The success criterion of the sub-goals has to be also analyzed.

(ISO, 1998; Wixon et al., 1997)

Some weaknesses to ISO9241-11 are that it does not tackle the viewpoint of learnability, which most of the usability experts consider as an essential part of usability (Abran et al., 2003; Nielsen 1993). The ISO standard also does not make any connection to the security questions relating to usability, even though including this connection to the definition of usability has a lot of support from the domain experts (Abran et al., 2003).

## 2.3 Security

The International Organization for Standardization defines security in the context of Information Security in their standard ISO 27002 (ISO, 2005) to consist of 12 different areas:

**Risk Assessment** - determining asset vulnerability;

**Security Policy** - management direction;

**Organization of Information Security** - governance of information security;

**Asset Management** - inventory and classification of information assets;

**Human Resources Security** - security aspects for employees joining, moving and leaving an organization;

**Physical and Environmental Security** - protection of the computer facilities;

**Communications and Operations Management** - management of technical security controls;

**Access Control** - restriction of access rights to networks, systems, applications, functions and data;

**Information systems acquisition, development and maintenance** - building security into applications;

**Information security Incident Management** - anticipating and responding appropriately to security breaches;

**Business Continuity Management** - protecting, maintaining and recovering business-critical processes and systems;

**Compliance** - ensuring conformance with information security policies, standards, laws and regulations

Of these 12 different areas, Access Control is the most relevant one for the scope of this thesis. Access control starts with identification, where the user makes a claim of his identity. The truth value of this claim has to be asserted before the user can be granted access to the controlled system.




The truth value of identification is determined in the process of authentication, where the user provides the service a trusted piece of information to verify his identity, and the service knows that only a legitimate user should have access to that information. Authentication process is presented with more detail in chapter 4.

Next step after authentication is to determine what of the areas user can access in the system and what kind of actions he can perform; the user has to be authorized. Authorization can be controlled by centralized administration (non-discretionary approach) or the owner of the information resource (discretionary approach). (Renaud, 2005)

Access control security of any given system can be divided to internal security and external security. Internal security is related to the system properties and functions and how well they are aligned with the rest of the system. External security considers the environment around the security system and actors related to it. Both aspects of security are important when considering an overall secure system, as they can either support or undermine each other. (Renaud, 2005)

## 2.3.1 Internal security



Predictable to:	Number available	Key Is:	Attack Type:	Authentication Key	Revealed During Entry
Anyone	$\leq 10^6$	Easy to Record	Keyboard tapper	Private Details Required	Full
Friends and Family		Easily Observed at Entry	Brute Force Research-Based	Private but User Decides	Part
No one	$\geq 10^{12}$	Impossible to Disclose	N/A	Not Private	None

Figure 4. Security dimensions (Renaud, 2005).

As seen in Figure 4, internal security can be divided to six different dimensions with varying security deficit. In practice these dimensions are highly interdependent and changing one dimension will certainly affect several others. But all of them still have different characteristics that have to be considered separately. (Renaud, 2005)

## **Predictability**

Predictability is a big issue in security, especially in authentication, as people tend to select weak passwords that are easy to predict (discussed further in section 3.2). Passwords selected by the user or generated by the computer have the highest potential predictability. Biometrics and system-generated recognition are the most unpredictable methods, but if the user can select the recognition pattern himself, it becomes as predictable as user-generated passwords. Cultural recognition, based for example to childhood memories, is at the middle of the scale; the information is generally known by only a few people, but it might be possible to uncover it with research-based attack.

## **Abundance**

Abundance means the amount of alternatives that user has when selecting his authenticating information. For example if the choice is limited to the recognized words of English language, the user has only 1 000 000 alternatives. On the other end of spectrum are graphical and cultural passwords, which have a theoretically unlimited amount of alternatives when used correctly.

Biometrics is very limited in abundance, as we have only two retinas, ten fingertips and so on. If biometrics is used in a controlled environment, abundance is not an issue. But in uncontrolled environment the lack of abundance and inability to replace compromised authentication may have serious consequences.

## **Disclosure**

The password or any other forms of authentication should not be disclosed to anyone; otherwise the reliability of authentication fails. If the user can easily record his authentication and it can be given to, observed or stolen by somebody else, the system is clearly deficient. The least deficient options are recall-based authentication scenarios and tokens that are based on non-disclosed shared secrets. However, the recall process can be observed and repeated, and the token can be given away or stolen, which can also be counted as a disclosure.

## **Breakability and crackability**

This dimension is defined by the amount of time, effort and money that the attacker has to spend to complete his attack and gain access to the system. Research-based attack to actually

know the user and his history is the most costly form of attack. Passwords that can be attacked with brute force and dictionary attacks are less secure. The worst points go to systems that are open to external observation like keyloggers and similar malware, which are really easy and efficient methods for attackers.

## **Privacy**

The system might want to record personal details to support the authentication or key recovery (e.g. in case of forgotten password). These details might either potentially compromise the security of other services if they are connecting to same information, or compromise user privacy by forcing him to share personal information. Biometrics has a maximum deficit, as it reveals very personal details to the system. In addition especially fingerprints are strongly associated with law enforcement and thus (mis)using them constitutes as an inherent privacy violation. At the moment most users do not have similar associations with other biometric system, but situation might change if for example retinal scanners would become more popular in the official context.

## **Confidentiality**

Authentication process is based on the confirmation, which the user is in possession of a pre-agreed key. The confidentiality-dimension is defined by how vulnerable that key is during the authentication process; if it has to be fully revealed, like in the case of alphanumeric password, the system has the least amount of confidentiality. Methods that reveal only parts of the key (like cultural recognition) or methods that use random responses signed with a shared key, thus keeping the key itself completely hidden (like SecurID token) are considered to be more confidential.

## **2.3.2 External security**

In addition to the internal security dimensions, every truly secure system has to be aligned with its environment. Aligning the system security with the environment requires taking into consideration a wide array of factors of accessibility, memorability, cost and external security. It is practically impossible to list the important individual factors as they vary in each environment, but some of the most important security factors are fairly universal: (Renaud, 2005)

## **Trust**

If the user trusts the person or organization that is requesting authentication, the internal security dimensions privacy and confidentiality become less important. The connection works the other way around as well, if the user does not know or does not trust the service provider, internal privacy and confidentiality become more important.

## **Security motivation**

This reflects how strongly the organization can motivate individual users to act according to the existing security practices. If the users have enough security motivation, the internal dimension of disclosure is still important but not as vital as with low user security motivation.

## **Auditing**

If system auditing is done in real time, it can trigger secondary security mechanisms when the system is compromised and thus minimize the damage. If there is no auditing, the internal dimensions of breakability and crackability become vital.

### 3 Balancing Usability and Security



Balancing usability and security has been a researched topic long before the term “cloud computing” was even conceived (Saltzer et al., 1975; Reid, 1991; Bishop, 2005). As securing any system essentially means limiting access to its information in one way or another, the issues of balancing usability, the ability for wanted users to access the information conveniently, and security, making accessing the information as difficult as possible for the unwanted users, has been a challenge during the whole intelligent history of the human race.

This chapter will introduce the theoretical background for balancing security and usability related to ICT systems. In addition to the actual authentication methods, which will be discussed in more details in chapter four, this chapter will also present the most important external factors affecting the authentication process.

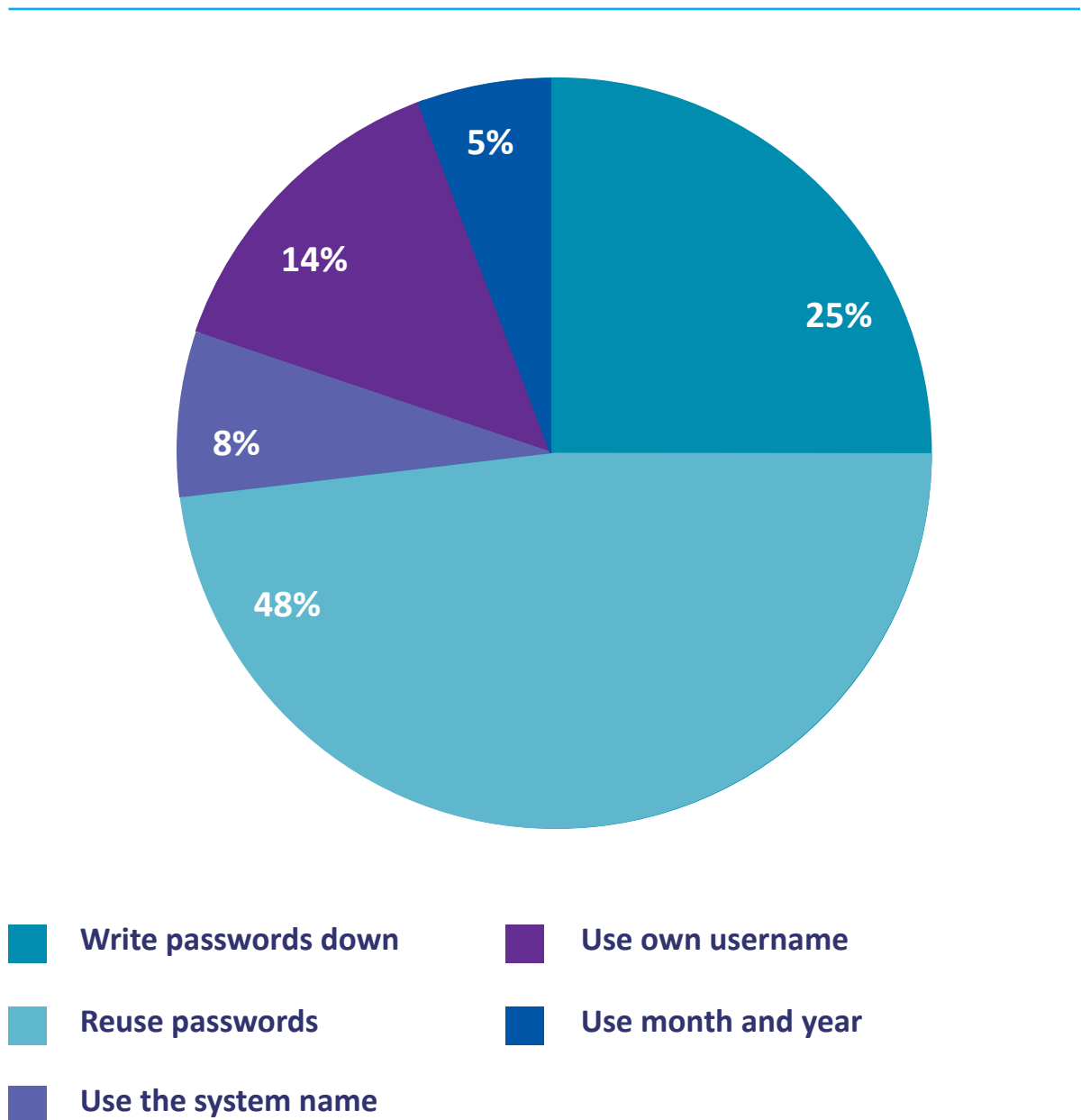
### 3.1 Passwords

For the scope of this thesis, the relevant starting point for analyzing the history of usability and security is the history of offline and online computer systems and their authentication. The most common and thus most researched authentication method in the era of personal computers has been the combination of a unique user ID and a password. The method consists of two stages: a public identification (user ID) to identify the user and a secret password to verify the ownership of the ID. Many of the phenomena observed with passwords are applicable with other similar authentication methods as well. (Adams et al., 1999).

In their article ‘Users are not the enemy’, Adams and Sasse argue that the human factor should be included in the design of the security mechanisms (Adams et al., 1999). They point to previous research (DeAlvare, 1988; DeAlvare et al., 1988) to show, that the users have a tendency of trying to avoid or go around the high security standards meant to assure password security (FIPS, 1985) when the users do not see the balance between security gains and usability hindrances. This kind of behavior might lead the security departments to classify all the users as inherently insecure or, even worse, as the enemy to be managed with even stricter limitations and by demanding for longer passwords (Adams et al., 1999).

Creating new, tighter technical rules that are against the users’ existing workflow has the complete opposite effect than intended (Renaud, 2012). Several authors point out, that when password requirements get too complicated, when the passwords have to be changed frequently, or the user has to use too many different passwords overall, the users will react against these changes. The cognitive overload will drive the users towards different coping methods (Table 1). These coping methods will erode the overall security, keeping up just the appearance of security towards the administrators. And it is not just the users; even the administrators and

experts start breaking their own rules when they think that the rules are on their way. For example, in his article *When Security Gets in the Way*, Norman (2009) tells a rule-breaking story to give a glimpse inside the minds of a roomful of the world's top security experts: they used stones to prop open several high-level security doors next to the auditorium to make toilet breaks easier during a security conference. (Renaud, 2012; Adams et al. 1999; Norman, 2009)



*Table 1, The popularity of different password coping techniques. (Renaud, 2012).*



## 3.2 Stealing passwords

Users themselves are not the only attack vectors against passwords. During the recent years, several big companies and social networks have lost millions of passwords to various attacks and data leaks. One of the biggest and most analyzed leaks was LinkedIn (Kamp, 2012). In June 2012 the company announced that 6 458 020 passwords had been stolen from them and published in a Russian hacker forum.

Luckily for LinkedIn and its users, the passwords that were published, were not in clear text format, but just a hashes of the passwords. A password hash is calculated with a hash function when the user creates his account, and only this one-way hash is saved to the system. The only way for outsiders to know what alphanumeric string created the hash is guessing, calculating hundreds of millions possible passwords with the original public hash function and comparing them to the stolen hashes. (Kamp, 2012).

No matter how efficient hashing algorithms or how much salting is used, all hashes can be cracked with enough time and computational power. But as people tend to use same passwords for multiple accounts, it is important to protect the passwords well enough to give them time to prevent the damage from spreading to other services when the password hashes get stolen.

As a positive result, these data leaks help the researchers to define the most common passwords and guide people to avoid these easily crackable alternatives. According to research by SplashData, the most common passwords in 2012 were “password”, “123456” and “12345678” (SplashData, 2012).

Big web services are also starting to understand that just passwords are not strong enough to protect the user data. The recent password leaks have hastened many companies like Google, Dropbox and several big online gaming companies to provide two-factor authentication for their users, and according to their public discussions, many other companies are planning to do the same.

## 3.3 Communicating with the user

There are no simple solutions for designing the balance between additional password security mechanisms, added difficulty and the insecure coping methods. However, there are some methods presented in the literature that will help to move towards a better balance.

Traditionally one of the cornerstones of information system security has been that the users know as little as possible about the system, so they would not be able to break it or tell outsiders about it. Also, most of the non-technical users might have a somewhat distorted view of technical security issues like levels of password entropy and dangers of dictionary attacks, and these misconceptions drive their actions to insecure practices. (Adams, 1999; Renaud, 2012)

In optimal situations, communicating with the user can solve both of these main issues; the security system itself does not necessary have to be changed at all. The first thing communicated to the user should be the basic rules in easily understandable format: how the system works and what a compliant and secure password is. The users should be provided assistance or feedback while selecting the optimal password. The users should also be provided with more secure alternatives than Post-It notes to store their passwords if, and when, the storing becomes necessary. (Norman, 2009; Adams et al., 1999)

Users might also need education about the data security to avoid accidental leaks. According to Adams and Sasse, the observed users easily identified the need for security with data that contained sensitive information about individuals, but it was a lot harder for them to correctly classify such business-critical information as customer databases or financial data. (Adams et al., 1999)

### 3.4 Punishing the users who break the rules

If and when the security breaches happen, it can sometimes be attributed to a single compliance failure of an individual user. In some cases (Renaud, 2012) the first reaction would be to punish the user or even terminate his contract. If the error was deliberate and showed high level of security neglect, this might be the right course of action. However, in some cases the user was just acting according to the company culture, and the culture itself was distorted in the security compliance. In this kind of cases the punishment would serve only as a short-term warning to the rest of the organization and the security would soon deteriorate back to the normal level. In these company culture-related breaches, it will be more effective to focus on company-wide education and instructions to raise the overall security level.

Worst course of action is to do nothing, or at least nothing visible to the users. This kind of non-action after security breaches tends to cause “it does not matter anyway” –type of attitude towards all of the security rules. The company-wide action also helps to adjust the users’ level of perceived threats closer to the real situation. (Renaud, 2012; Adams et al., 1999)

## 3.5 The weakest link?

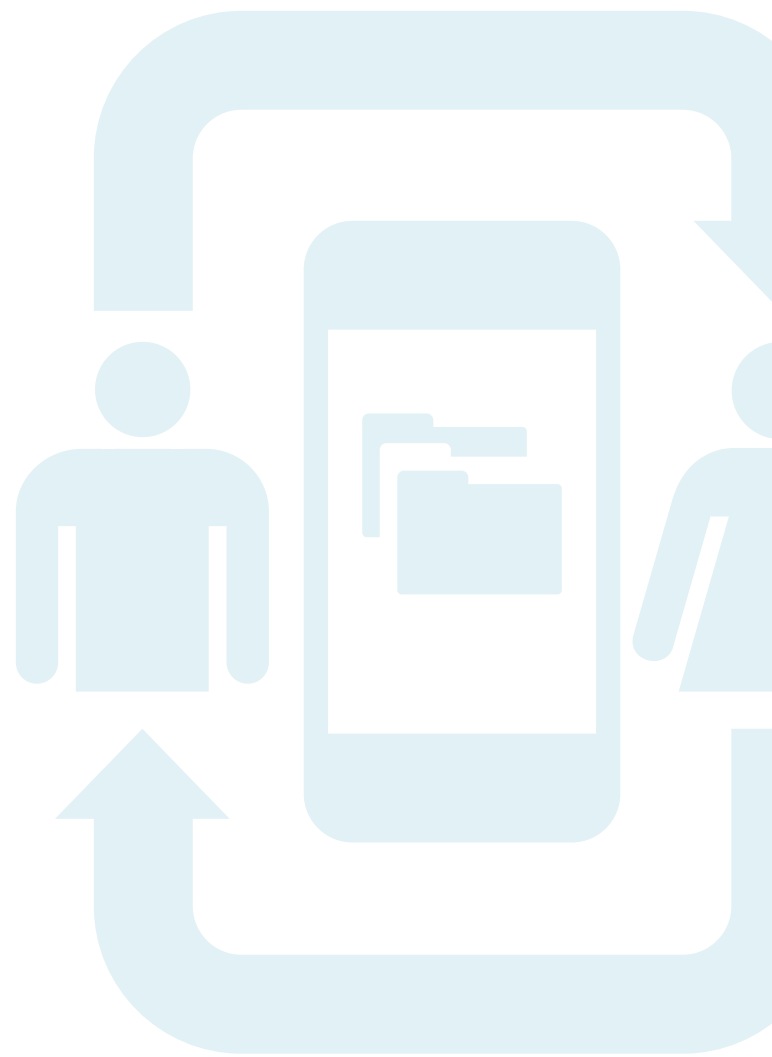
Most of the security breaches to computer systems are not done to computers; they are done to humans (Sasse et. al, 2001). The first of such attack vectors is towards the users themselves and their coping methods. The attackers can use the inbuilt flaws of the security setups, like too frequent password changes that lead the users to write their passwords to post-its, as a leverage to gain access to the system (Sasse et. al, 2001).

The second possible attack vector is to utilize more sophisticated social engineering tactics to con the legitimate users into giving them the access voluntarily. According to a general definition, social engineering is manipulating natural human tendency to trust others (Granger, 2001). In one of his examples, Granger (2001) tells a story about a group of social hackers that were able to gain a complete access to a big company's well-protected network with a combination of social engineering and security flaws; they pretended having lost their keys and security cards and friendly employees helped them by letting them into the building. Next they got into an executive's office and used the few basic facts they had studied of him to con the network password from the IT support. After that they were able to extend to full access to the system with regular hacking software.

Different kinds of password recovery systems are also one of the most common attack vectors to any system that utilizes the option. In some cases the answers to the recovery questions like "what is your mother's maiden name" can be found easily through social media or with a few Google searches (Bonneau 2010). Some services like highly security-focused email provider Hushmail externalized the problem by encrypting the account content and not storing the encryption key themselves. When the user forgets his password, he might be allowed to wipe the whole account and start from zero with the same name, but all the stored content like credit cards numbers would be automatically wiped and thus unavailable for attackers. This would also destroy all the data for the legitimate users, so there still is some potential for misuse or unintentional damage. Some online merchants like BestBuy offer a mixed approach to the issue by wiping the most valuable data like credit card info, but retaining some info for the convenience of the customer. (Bonneau, 2010; BestBuy, 2013)

Another alternative for a security breach is to use social engineering skills against the customer support and have them unknowingly do all the hacking. For example in a social hacking exploit used against Amazon.com in late 2012, the attackers were able to bypass the adequately password-protected online store features by contacting the customer support with a few data points found from social networks; the content of the order from user's twitter post and basic user details from the his social media profiles. With those details the attackers managed to convince the customer support into thinking that the original orders were lost during transport and that the replacements should be sent to their address. (Cardinal, 2012)

## 4 Authentication methods and situations



This chapter takes a look into three different categories of authentication methods and their suitability for cloud service authentication. Based on the different properties of authenticating factors, authentication has been traditionally divided in three categories: something you have, something you know (memometrics), or something you are or can do (biometrics) (Cohen, 1997; Renaud, 2005). Each of these categories can be used alone to authenticate a user, or then they can be used in sequence for two-factor or multiple-factor authentication scenarios for added security, but also potentially reduced usability. This chapter will take a closer look into these authentication methods and some of the most common technologies from each method. The chapter will also present a fourth, emerging category, “somebody you know”, which is designed on top of the social layer and human connections.

The chapter will also examine several alternatives for sharing authentication and single sign-on, technologies designed to reduce the amount of different login accounts for the users.

In the context of business cloud and desktop virtualization, there are three most common authentication scenarios that the end users will encounter. These scenarios were used as a starting point to select and evaluate the authentication methods to be introduced in this chapter, and further when selecting the methods to be included in the usability study that is introduced in chapter 5.

**Scenario 1:** Using the virtual desktop through the company network or separately authenticated VPN, with a tightly controlled company-owned PC.

**Scenario 2:** Using the virtual desktop through open network at a secure location (e.g. the office, home) with a self-purchased PC (or a loosely controlled company-owned PC)

**Scenario 3:** Using the virtual desktop through an unknown network with an end device owned by a third party from anywhere around the world, e.g. from internet cafe during a vacation.

## 4.1 Something you know

Knowing-based authentication includes solutions like passwords and similar learnable, repeatable and copyable information. As the intensity of brute force attacks is growing on par with the computational power of normal PC’s, this traditional cornerstone of authentication is starting to lose its value as a single authentication method. As the brute force attacks become easier to implement, the required password complexity to deter them increases. The situation is already getting near to the point where the required complexity of a password determined to be “relatively secure” becomes impossible to remember for an average person. (Coskun et al., 2008)

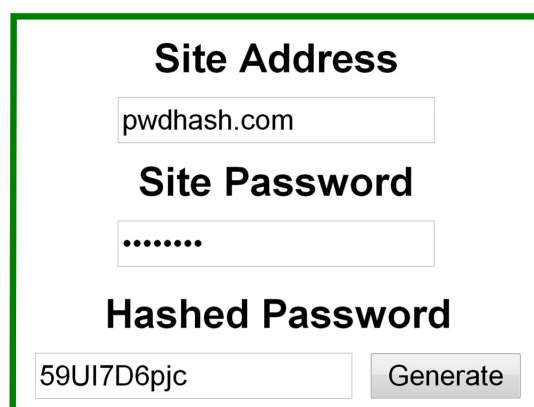
## 4.1.1 User ID and password

A combination of a public identification (user ID) and a secret alphanumeric string to authenticate a user has been the most commonly used method in the history of ICT security (Adams et al., 1999). As the computational power is getting cheaper, the passwords have to get longer and more complex in order to offer adequate protection. And a long password alone is not enough if it is used in two or more services; if one service is hacked then the compromised password can be used to break into all the other accounts. During the past two years alone, 280 million encrypted passwords have been published for everyone to see, usually in connection with a large security break to popular Internet services. A comparison between these encrypted password leaks showed that 49% of the users had reused their passwords in two or more of the hacked sites. (Honan, 2012)

## 4.1.2 PwdHash – Service-specific passwords through hashing

As mentioned above, one of the issues with the password infrastructure is creating unique, service-specific passwords that are complicated enough to meet all the security criteria and still remembering all of them. One possibility to solve this issue is to use a single cleartext password and using a secure algorithm to combine it with the domain name. Stanford Security Lab developed one version of this approach, called PwdHash (Ross et al., 2005). Using PwdHash to combine an example domain

`http://pwdhash.com` with a simple and insecure password “password” provides a unique and a lot more secure hashed password “59UI7D6pjc” as seen in Figure 5. A big part of the PwdHash project was to improve the usability of the hashing solution by developing a browser extension to do the hashing automatically when the user presses F2-key or precedes the password with a string @@. PwdHash adds password entropy significantly with a minimal change to the user’s login process and no changes to the server configuration.



**Site Address**

**Site Password**

**Hashed Password**

Version 0.8 ([more versions](#))  
Tip: You can save this page to disk.

*Figure 5. PwdHash online interface.*

## 4.2 Something you have

Having-based authentication means that you prove your identity with a physical object you have with you. This can be built especially for authentication (like RSA tag or a key) or authentication can be considered as a secondary function of the object (like a mobile phone). Confirming the ownership of the authentication object is not part of a having-based authentication, so anyone who has access to the object can use it to authenticate himself with the exact same authorization than the original owner. (Renaud, 2005)

### 4.2.1 RSA SecurID – hardware token

RSA SecurID hardware token, manufactured by EMC (EMC, 2013), is a physical device that contains a lock and a secret key. When the two are combined with a cryptographic function that includes the date and time of the creation, the product is a numeric code on a small display (Figure 6). The user has to manually type the code to the authenticating application, which checks the code validity from RSA servers. The authenticating RSA servers know the secret key stored at the user token and the authentication time; based on these the authenticating server performs the same cryptographic function than the user token. If the values entered by the user and calculated by the server match, user is authenticated as the owner of the actual token. (Renaud, 2005)



*Figure 6. RSA SecurID SID800 token without USB connector (Ochro, 2008).*

## 4.2.2 Software token

The cryptographic functionality of the software token is identical to any hardware token, like RSA SecurID which is presented in chapter 4.2.1. The difference is that the software token runs on a shared hardware, like a PC or a smartphone and is installed like any other software on that platform. After the installation, user can either import his own personal secret key, or the software connects to the authentication server and generates a new shared secret automatically. The key is then stored securely on the device without any needs for connecting the authentication server during subsequent authentication processes. The software token presents a similar code (Figure 7) than a hardware token, which has to be typed to the authenticating application by the user. (Renaud, 2005; NordicEdge 2013).

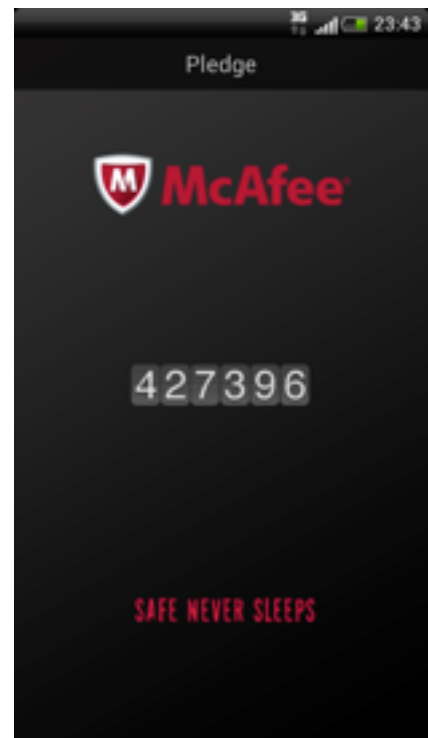


Figure 7. NordicEdge Pledge, a software token.

## 4.2.3 SMS token

In SMS token system, the authentication factor is the MSISDN (ITU, 2010) of the user, which is saved to the authentication server and associated with a certain user. The SMS authentication is initiated by the user identifying himself or logging in with a first-factor authentication like alphanumeric password to the authenticating service. This prompts the authentication server to send a SMS message with a single-use authentication code to the MSISDN associated with the user. When the user writes the received code during secondary authentication, he is assumed to be in possession of the device connected to the MSISDN. (NordicEdge, 2013)

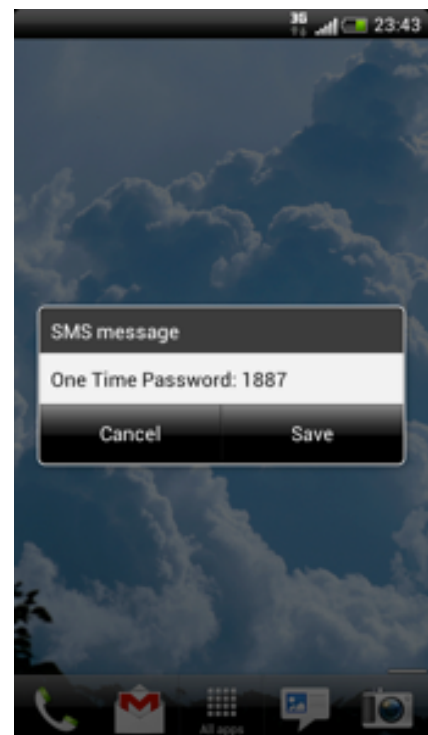


Figure 8. SMS token.



## 4.2.4 Email token

The email token is cryptographically identical to the SMS token presented in chapter 4.2.3. The difference is that the pre-defined delivery route is an email message instead of a SMS message. (NordicEdge, 2013)

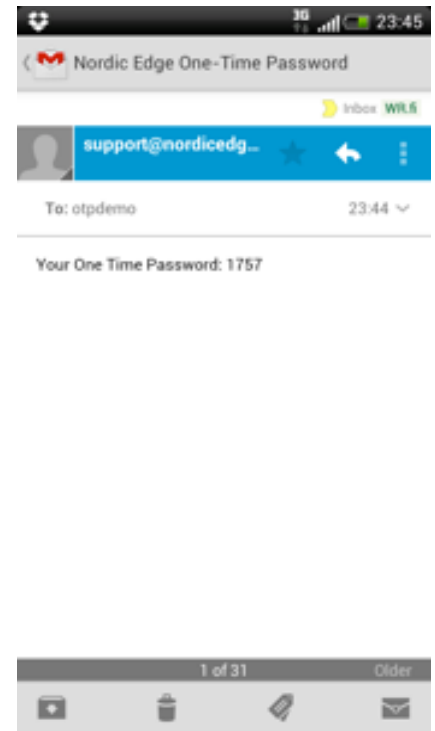


Figure 9. Email token.

## 4.3 Something you are

The third authentication category is about being or doing, and it consists of the indistinguishable physical or genetic properties of a person. These biometric identification methods are usually fast to perform, always available and have a relatively low theoretical False Acceptance Rate (FAR, accepting wrong users). However, on the flipside of low FAR, the system might have a relatively high False Rejection Rate (FRR, not accepting the real user). High FRR makes a system highly unusable and might even cause catastrophic problems if the authorized users fail to authenticate themselves in critical situations (Matyas et al., 2003).

Biometrics is a challenging for cloud access, as it usually require a separate scanner or other device to read the analog biometric input into a digital format. In addition, most of the biometric characteristics are relatively easy to forge in an uncontrolled environment; for example simple face recognition systems can be fooled with a photograph of the person.

These issues can be resolved by requiring a controlled environment, but this usually negates the mobility benefits of the cloud computing and might be inconvenient for the user. However, controlled biometrics has a potential of huge amount of easily transportable and highly personal authentication information, thus it is already used in high-security environments like border control or securing physical access to high-profile facilities. (Coventry, 2005)

### **4.3.1 Fingerprints**

Using fingerprints as an authentication method is done via a fingerprint scanner, which is either built in to the login device or temporary attached as an add-on device. The scanner reads the ridge pattern of the finger and converts it to a digital format according to pre-defined specifications. This digital representation of the finger is then compared at the authentication server, or sometimes even locally, to the comparison sample recorded during the user enrollment. All ten fingers have a different fingerprint pattern and they can be used in authentication individually or consecutively to add entropy. In some implementations the user can also add backup fingers (e.g. from his left hand) to prepare for potential physical damage rendering the primary fingerprints unreadable. (Maltoni et. al., 2009)

### **4.3.2 Face recognition**

Face recognition applications work in three main stages. First the face has to be digitalized with a camera, like a standard webcam or a single-purpose authentication camera.

The second step is locating the face in the image; if the image has a single face as a major element and the contrast to the background is clear, this is an easy task. If the image has multiple faces (e.g. in a crowd of people) or a lot of movement, this task becomes significantly more difficult.

The third step is for the software to analyze the spatial geometry of the face, like the distance of the eyes and mouth. These results are then compared to the face template saved from the user during the enrollment process to confirm the authentication. The false acceptance rate and false rejection rate of the face recognition has to be adjusted carefully to fit the use scenario. (Coventry, 2005)

### **4.3.3 Iris scanners**

The iris scanner is a high-precision camera that analyzes the vein pattern in the iris, the colored part surrounding the pupil in the eye. The scanner needs a precision camera and alignment system that guides the pupil to a right position for imaging. Each human has two distinct iris patterns and the possible entropy in the vein positioning makes it extremely improbable to have two matching iris pattern in the whole human population. (Weaver, 2006)

### 4.3.4 Voice recognition

Like all biometrics, voice recognition authentication consists of two phases: enrollment and verification. In enrollment the voice sample of a validated user is saved to a database to be used as a comparison for all future verification attempts. The voice authentication can be either text dependent or text independent. In text dependent the voiceprint is a pre-defined sentence like users name or id number. Text-independent voice authentication can be done with any voice sample, but achieving good results requires a lot longer samples at enrolment and verification. The minimum sample rate for some text independent systems is 30 seconds, and even this does not guarantee high success rate in varying conditions. (Gunson et al., 2011; Trewin et al., 2012)

## 4.4 Somebody you know

In addition to the three classical authentication categories, the concept of “somebody you know” as a fourth authentication category has been gaining attention. This concept takes the age-old approach of human authentication through mutual acquaintance to the era of computer security and location-independent social networks. There are several technical alternatives for building a social authentication system, but the conceptual idea behind all of them is to have familiar people to verify the user’s identity as a part of the authentication process. This kind of authentication is usually a lot heavier process, as it needs active participation from at least one other person who can vouch for the authenticating user. Because of the unknown availability of any potential authenticator, it can be difficult to estimate the time needed for the authentication. Because of these limitations, most of the current setups use human authentication as a backup to other methods, e.g. for password resets, or as one additional factor in ultra-high security applications. (Brainard et al., 2006)

## 4.5 Sharing

In systems and environments where users have to log in to multiple computers, software and websites, implementing shared authentication or a single sign-on solution is usually the most effective way to improve the user experience without compromising security (Anchan, 2003).

Shared authentication means that the user has only one account, which he can use to access all the organizational resources that previously needed to have separate user accounts. In shared authentication the user can use the same credentials, but he has to log in manually every time.

With single-sign-on, the manual authentication is required only once, after which the user is logged automatically to other services via single sign-on management system.

Implementing shared authentication or single sign-on can also increase the potential damage that one cracked or leaked user account can cause, so it is usually recommended to pay additional attention to the account security.

### **4.5.1 Corporate systems**

There are several technical alternatives to implement shared authentication and single sign-on. In corporate environments one of the most common alternatives is to extend the reach of the main user database, usually Microsoft Active Directory, to authenticate users from a wide range of services (Blezard, D.J., 2002). This can be done with several standardized protocols, most common one being Lightweight Directory Access Protocol, LDAP (IETF, 2006)

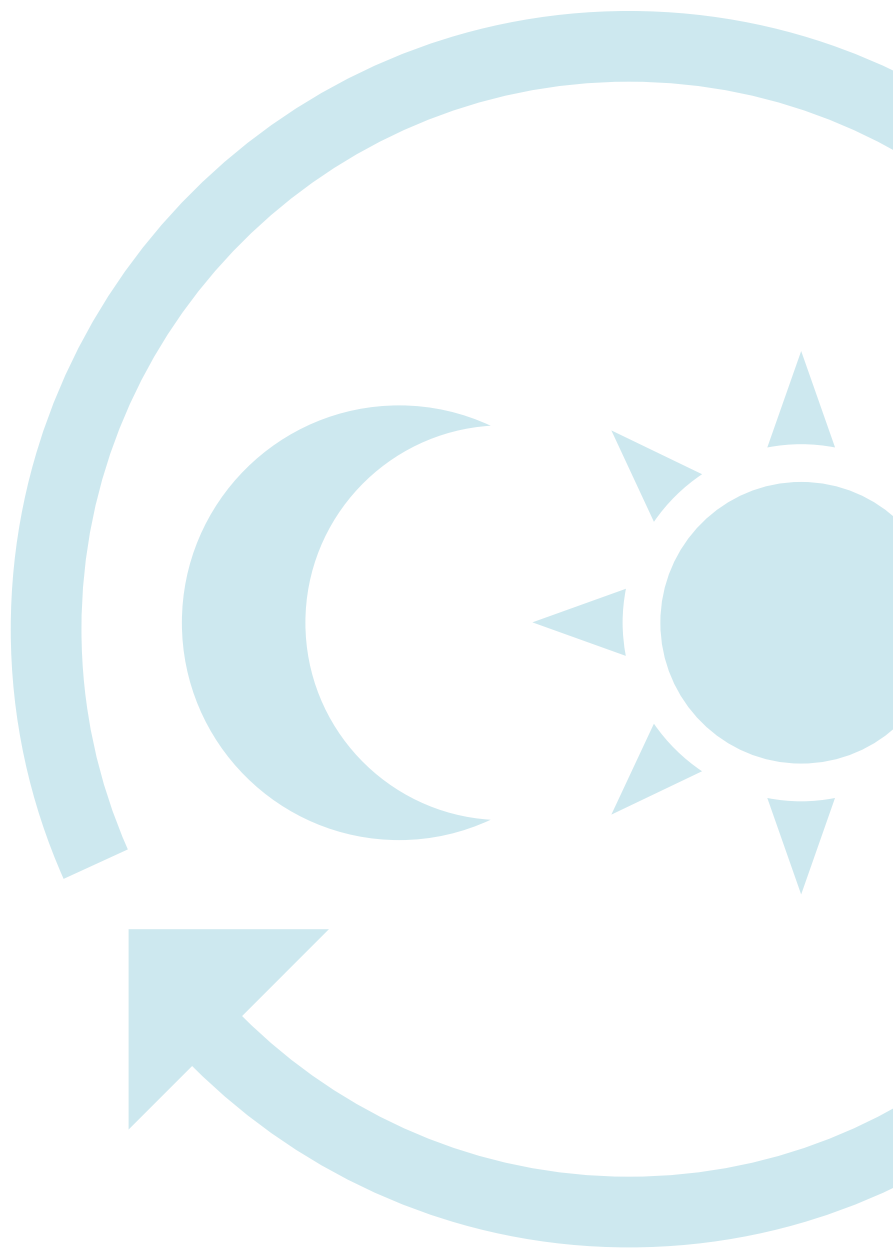
### **4.5.2 Online APIs**

In web-based environments users can achieve single sign-on to a wide range of services with open implementations like OAUTH or OpenID (Kaila, 2008). There are also vendor-specific solutions like Facebook Connect that rely on the existing user base of the primary service (Ko, 2010). The technical implementation of these three solutions varies, but the end result in all of them is nearly identical: the user can use his existing account to sign into a new service. The new service authenticates him from his old account, e.g. Facebook, via the predefined API.

### **4.5.3 TUPAS in Finland**

In Finland, most eCommerce providers and many public institutions like Kela, the social insurance institution of Finland, are using TUPAS as a shared authentication solution. TUPAS is a proprietary authentication solution developed in Finland and currently provided by all major Finnish banks. TUPAS allows the sharing of inherently secure Internet banking authentication to other high security logins. (Rissanen, 2010). Some big organizations also use the TUPAS authentication as a backup for primary account password recovery, as it is considered secure enough method to identify a person. For example the students of Aalto University can create and recover their University-wide primary password through a service that utilizes TUPAS (Aalto IT, 2013).

## 5 Empirical study



This chapter will introduce the designing and construction of the empirical study. The study progress and results will be introduced in chapter six. The empirical study was designed to evaluate authentication preferences of business cloud service users. The study follows the steps of usability testing methodology defined by Cranor et al. in the book “Security and Usability” (2005) and the structure is further based on previous research in evaluating the balance of usability and security (Weir et al., 2009). This chapter will present the construction of the empirical study, following the five steps slightly modified from Cranor et al. to better match the study structure by Weir et al.:

1. Purpose and scope definition. Defining the aims of the test (e.g., comparing the usability of two types of devices) and set the test’s limits.
2. Context and roles definition. Defining the context for the experimental scenario, including the simulated environment, user roles and the tasks they need to achieve. Each role must be specified clearly, including the possible actions of a supervisor.
3. User selection. Defining the selection criteria of users based on the selected context and aims of the test. The user sample has to be wide enough to assure statistical significance.
4. Task definition. Defining the set of tasks to be executed by each user (sequence of steps, input data and output data).
5. Measurement apparatus design. Choosing a set of metrics and specify their relationships with the usability attributes. Each metric has its own name, description, scale, and procedure to collect the raw data and to compute the measurement.

## 5.1 Purpose and scope definition

The aim of this study is to compare three alternative two-factor authentication methods commonly used in cloud service authentication and answer to the research questions defined in the beginning of this thesis. The main focus of this study is in rq3 and it will probably produce some additional information for rq2 as well. No additional information for rq1 is assumed to be found during the user study.

**Rq1** Identify a) the common authentication methods used in business cloud authentication at the moment and b) emerging new authentication methods suitable for the purpose.

**Rq2** What are the most important factors, in addition to the authentication method itself, that are affecting the security – usability –balance of the entire authentication process and how they can be optimized for the business cloud authentication?

**Rq3** How the usability and security aspects of authentication methods affect the user preference in method selection?

From the scenarios introduced in chapter 4, this usability study will focus on the scenario that fits best with the intended context, scenario 2.

**Scenario 2:** Using the virtual desktop through open network at a secure location (e.g. the office, home) with a self-managed PC

## 5.2 Context and roles definition

The scenario is set up to evaluate three different delivery methods of one-time passwords (OTP), defined with more details in sections 4.2.2 – 4.2.4: SMS, email and mobile software token.

The social context aims to be as realistic as possible for the intended user group, graduate students with work experience, and utilize the real test environment, school premises, as part of the context. The scenario is further defined to support the Scenario 2 defined in chapter 4: open network, relatively safe environment and self-controlled PC.

Each participant is told that his employer has gotten a new DaaS solution and will be moving all the work tasks to that environment. Now the environment is in testing phase and the user can try all of the available authentication methods and select one of them to be used with his account. When the system is taken into production, the selected method cannot be changed easily, so the user has to think his options carefully.

This scenario aims to get the users to better relate the authentication solutions to their personal work context. This effect is further strengthened in the account creation phase; in the beginning of the study each user creates a test account with his personal phone number and email address. The personal details are not used for anything else than OTP delivery, but the test users still have an alternative to use a dummy account if he does not want to use his personal information.

The active participants of the test will be the user and the supervisor (experimenter). The role of the supervisor will include:

- Conducting the pre-questionnaire
- Briefing the user for the tasks
- Acting as a customer support during the test
- Conducting the debriefing phase

**Create an Account**

1. Create an Account | 2. Login With Two Factor Authentication

First you need to create an account to be able to use the demo. It is important that you provide correct mobile number as it will be used for SMS passwords. Country code will auto fill on selected country.

**Note: This is the same account as for the self service demo. Go to login**

First name:

Last name:

Email:

Password:

Confirm password:

Country:

Mobile number:

Company:

Code (optional):

**suter** **100%!**

Type the two words:

reCAPTCHA™ stop spam. read books.

**Create** | Cancel

Figure 10. Creating the test account.



## 5.3 User selection

The usability study will be conducted with six users who are at the last stages of their Master studies in Aalto University. They should already have a moderate amount of relevant work experience on their own fields and some of them might already be familiar with two-factor authentication in a business context.

## 5.4 Task definition

The study will consist of four phases:

### **Pre-questionnaire** (Appendix C)

The pre-questionnaire will record the relevant background info and previous experience with cloud services and strong authentication solutions. The pre-questionnaire is done with a Google Docs –form, which facilitates easy data handling after the study.

### **Briefing**

After completing the pre-questionnaire, the users are briefed with the test scenario and given the task description. They are also told about the possibility to use the supervisor as a customer support if needed, but discouraged to do so with any minor incidents.

### **Execution**

User starts the test by creating an account for himself and providing the details needed to deliver the one-time passwords to him (Figure 10). After creating the account, user logs in with his email address and newly invented password.

The user is then presented with three alternative methods for the second factor of the authentication method, from which he selects one (Figure 11). The order of the method is randomized before each test in order to minimize the arrangement bias. After the authentication is successful, the supervisor presents a short questionnaire (Appendix D) to the user about the tested method. After the questionnaire, the user is instructed to log out and log back in with the next method in the randomized list, repeating the same process until all the methods are tested.

### **Debriefing**

At the end of the test, users will be given a debriefing interview.

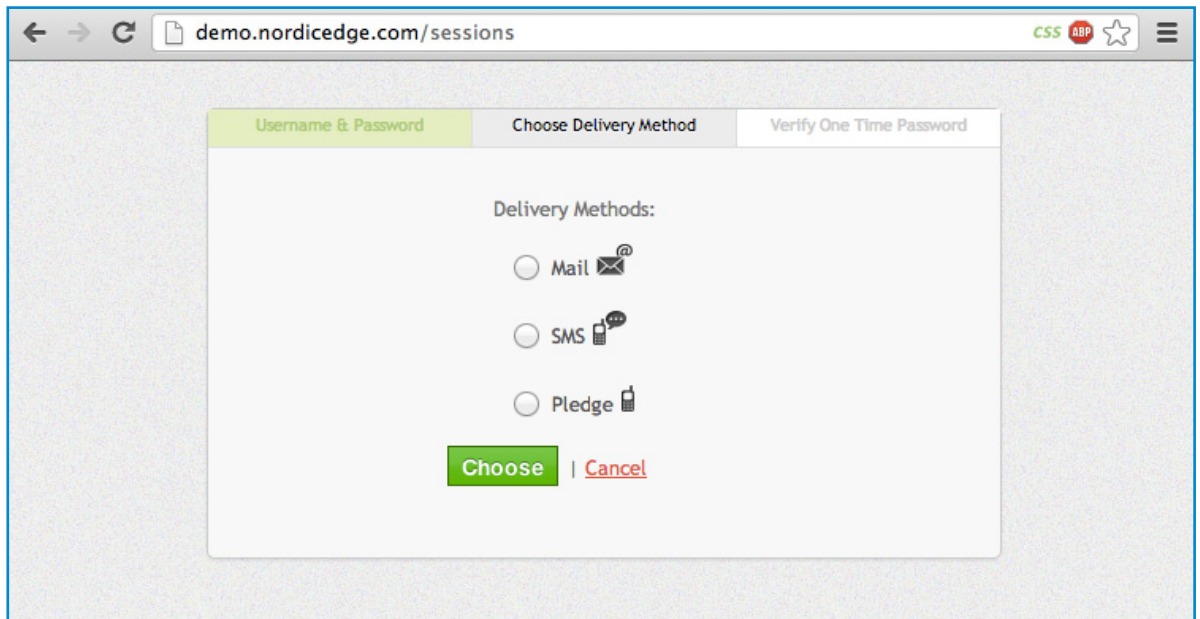


Figure 11. Selecting the second factor for the authentication.

The user is then presented with three alternative methods for the second factor of the authentication method, from which he selects one (Figure 11). The order of the method is randomized before each test in order to minimize the arrangement bias. After the authentication is successful, the supervisor presents a short questionnaire (Appendix D) to the user about the tested method. After the questionnaire, the user is instructed to log out and log back in with the next method in the randomized list, repeating the same process until all the methods are tested.

### Debriefing

At the end of the test, users will be given a debriefing interview.

## 5.5 Measurement apparatus design

The study will focus on the definition of usability by ISO 9241-11 (ISO, 1998), presented with more details in section 2.2.1 of this thesis: the standard measures usability with achieving the goals from three axes: Effectiveness, Efficiency and Satisfaction.

Efficiency will be measured by manually timing the whole login process for each authentication method. The timing will begin once the user starts typing his email address and ends when the first landing page is visible after a successful login.

Effectiveness will be measured in terms of task completion, amount and seriousness of task-hindering issues and amount of help requests from the supervisor.

Satisfaction will be measured with attitude questionnaires after each authentication method. The attitude questionnaire is adapted from previous studies (Weir et al., 2006, 2007, 2009), consisting of 18 statements about usability-affecting factors (Schneiderman et al., 2004), each measured with a 7-point Likert scale (Likert, 1932; Kline, 1999). The questionnaire includes an equal number of positive and negative statements in random order to create a counterbalancing effect, as it is easier for a human mind to agree than disagree with question statements (Colman, 2006). For the further analysis, the scoring of the negative questions was inverted to be aligned with the positive question set. The questionnaire is shown in Appendix A.

The users will also be asked to rank each method, overall, on a 30 cm scale, in which 0 cm is “the worst” and 30 cm is “the best” according to their own preferences. The same ranking scale will be also used for two other factors of the methods: perceived security and convenience of the methods. Figure 12 shows the situation after one of the participants had completed the evaluation.



Figure 12. Ranking methods on a 30 cm scale from worst to best

## 5.6 Technical setup

The test setup is built with the live authentication demo by a Nordic Edge, a McAfee-owned company that specializes in secure authentication products. The demo setup is built around three Nordic Edge products, One Time Password Server, Password Self Service and Mobile Software Token Pledge. The demo was available through URL <http://demo.nordicedge.com/> in January 2013, but has been since shut down.

The demo setup will allow all the test users to create their individual accounts and use their personal mobile phone and email accounts as authentication delivery methods during the user study (Figure 10). When using the demo setup, the users are logging into a web application that has no other technical functions than authentication. (NordicEdge, 2013).

The intended main function of the demo is to introduce Nordic Edge solutions to potential new customers, and as a result the demo website includes several web elements that are not related to the authentication process. To make the authentication experience as realistic as possible, the excess elements were filtered out during the study by manipulating the Cascading Style Sheets (CSS) of the demo on the usability study workstation. The situation before and after the filtering is presented in Figure 13.

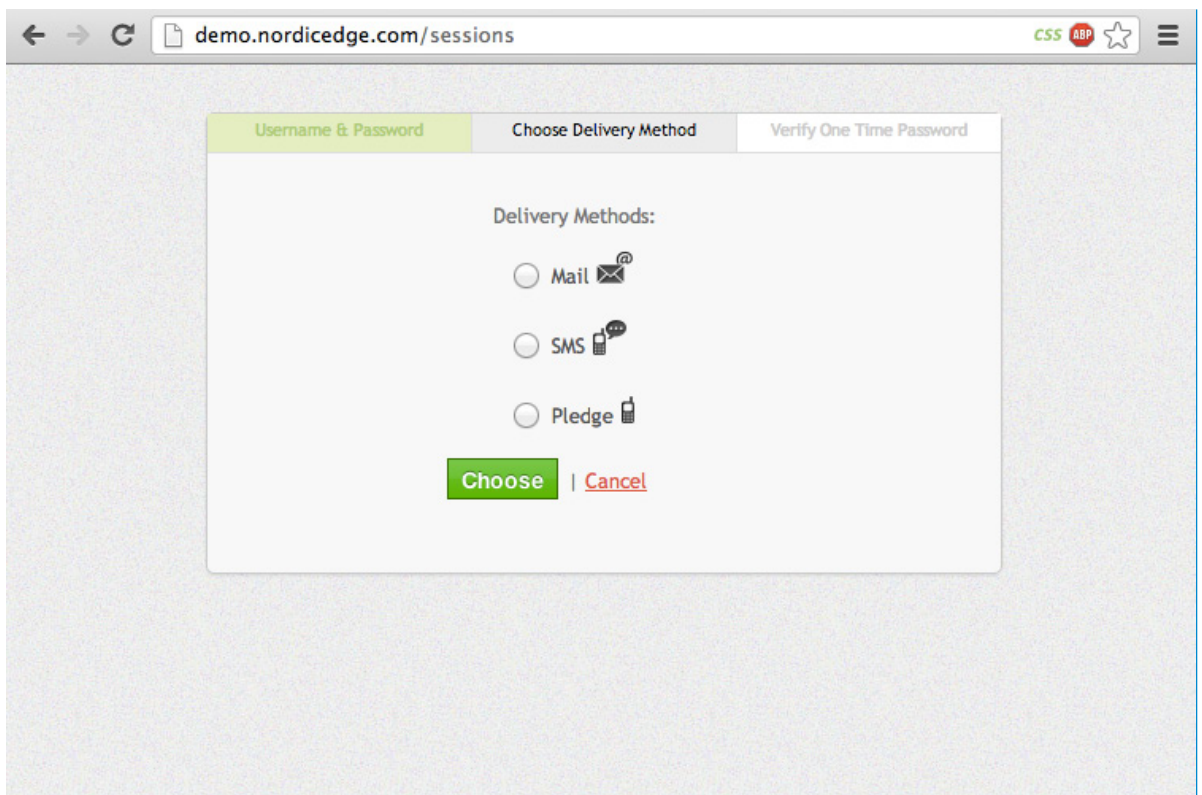
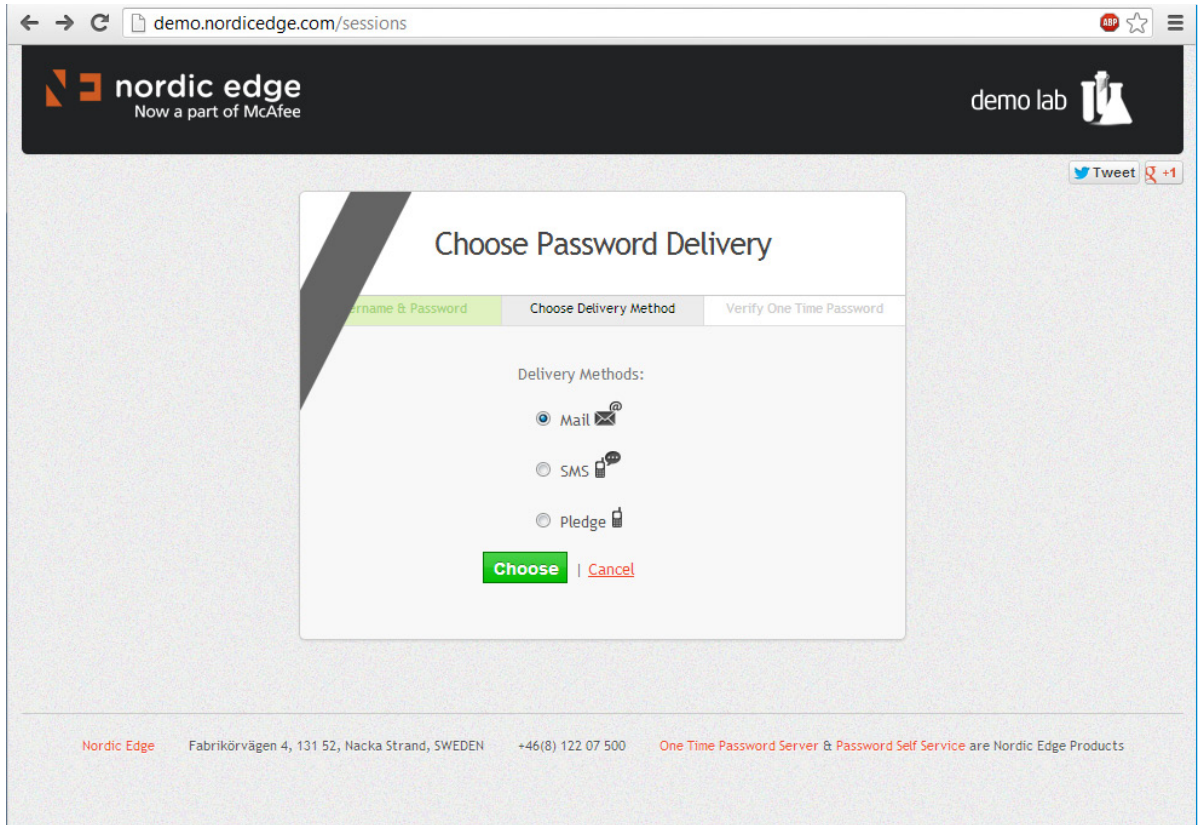


Figure 13. Live demo <http://demo.nordicedge.com> before and after filtering out the unnecessary website elements with a CSS editor.

## 5.7 Technical setup alternatives

The main purpose of this usability study was to compare the three different authentication methods and the demo setup by Nordic Edge was a good fit for the focus. However, in the real business cases the authentication is planned as a gateway to the actual services. To actually implement and test a setup that includes all the elements of the real business cloud environment, one has two choices:

- 1) Conduct the usability study in a real environment and modify it as needed; or
- 2) Build a realistic business cloud environment for the testing.

Conducting the tests in a real environment and getting the permission to modify the security settings for the test proved to be practically impossible. And even though it would have been possible, even a really well-prepared study would have caused a potential security and functionality risks to the environment and led to moral and monetary responsibilities for the study organizer.

Building a realistic business cloud environment for the testing would have been possible, but it would have included building a lot of background services, all of which would have stayed invisible to the test users during the usability study of the authentication process. And still, the end result would have been indistinguishable close to the demo setup in the selected alternative. This chapter will present a plan for building such an environment to give an example of the business cloud system where these studied authentication solutions could be used. Because a detailed plan of such system would be almost a thesis in itself, some of the technical details are omitted. The system design is based on the technical documentation by Citrix Systems (Citrix, 2013) and personal experience from building similar systems.

### 5.7.1 Deciding the platform

For the past two or three decades, one would have started with a question about what kind of server should be bought for this kind of setup. However, during the past few years IaaS (Infrastructure as a Service) platforms have grown up in popularity and functionality to be the most feasible alternative for many kinds of environments. This is especially true for a small-scale test setup like this, needed only for a limited time. Thanks to scalable pricing, increases in average networks speeds and many other benefits, the compatibility of IaaS as a platform building enterprise cloud services is increasing all the time (Sripanidkulchai, 2012). Of course there are still many situations where a dedicated physical server is still a better alternative, but the detailed analysis of the differences falls outside of the scope of this thesis.

On the vendor side the obvious choice for the implementation of this thesis was IBM's SmartCloud Enterprise (SCE), enterprise-class IaaS service that is a part of IBM's larger SmartCloud framework. The main reason for the selection was that the SCE platform and support resources were easily available, as IBM was the sponsor of this thesis. As IaaS services are planned to maximize compatibility with the existing infrastructure, the planning and implementation would have been nearly identical for all the other big IaaS services like Amazon's EC2, Microsoft's Azure and many others, with possible service-specific technical limitations.

## 5.7.2 Deciding the software components

As stated in the thesis introduction, the focus for the practical implementation is in the Citrix Systems' products. The selected Citrix components for the test setup were Citrix XenApp and Citrix Storefront. For a hardware server setup it would have been possible to install a XenServer hypervisor platform to manage and share the server resources to several virtual computers, but for this setup that function is handled by SCE as a part of the IaaS implementation.

### Citrix XenApp

XenApp is Citrix's software virtualization app, which can be customized to provide a DaaS experience by combining the individual virtualized software launchers on top of one application running the desktop experience with components of Windows Server 2008. Without the customization XenApp could be considered a pure SaaS (Software as a Service) platform. However, after the customization the end result and user experience is fully compatible with a pure virtualized desktop. Citrix would also have a product for pure desktop virtualization, XenDesktop, which could publish a full image of any popular Windows OS. The main reasons for selecting XenApp over XenDesktop were licensing issues and small size of the planned software setup.

With the current license agreements, Microsoft requires a full OS license for every virtual computer running a desktop OS (Operating systems like Windows 8, Windows 7, Windows Vista and Windows XP). This makes the underlying idea of any cloud service, dynamic resource scaling, really difficult to implement and introduces additional license costs. However, with XenApp, it is possible to share the Windows Server 2008's desktop as an "application" to several users, and this is covered in Microsoft's server license.

The size of the setup environment and the amount of needed resources was another deciding factor. The whole test setup was implementable on XenApp with only three Windows 2008 R2 servers, described with more details in the next section. A full XenDesktop setup with similar functionality would have required at least five Windows 2008 R2 servers and an additional virtual machine instance for each of the virtualized desktops.

## Windows 2008 R2

The recommended installation platform for all the software components in this setup is Microsoft's server operating system. Currently the newest supported OS version for most of the components is Windows 2008 R2, which can be installed easily on the SCE IaaS platform. There are several server roles and software components to be installed on the servers, some of which are not compatible to be installed on the same server instance. To increase the system capacity, these roles could be shared to multiple servers. Or the individual roles could be divided between several servers, called a cluster, to support more users. However, as this is a test setup just for a few users, the roles can be combined on a minimum setup requiring three separate Windows 2008 R2 server instances from the SCE cloud.

- The first server will host the Active Directory domain, which connects the servers and acts as a user database for the first- and second factor authentication (see details from section 4.5.1). This server also hosts the license server for the Citrix products.
- The second server will host the XenApp setup, consisting of the server components and the virtualized applications to be published. In addition it will host the Citrix Web Interface, a service that allows the users to connect and authenticate themselves to the XenApp server with their Active Directory accounts. This server will also host all of the background services needed for these functions.
- The third server hosts the software setup for the second-factor authentication, which in this test setup is NordicEdge One Time Password Server, allowing the authentication with SMS, email or a Pledge client, among other available methods. This OTP server uses the Active Directory on the first server as a user database, thus the two servers are connected with standard LDAP protocol.

### NordicEdge One Time Password Server

One Time Password (OTP) Server is a product of NordicEdge, a company that is currently owned by the security giant McAfee. OTP server is one of several similar authentication server products, which connects to other services and provides a wide array of additional connectivity and authentication alternatives for them. OTP Server was selected because its market share and previous positive experiences of the author. The end-user experience of OTP server is identical to other similar products as all the end-user parameters (message content, code length and validity time) are fully configurable.

In this setup the OTP server uses the Active Directory (AD) database of the setup to store the information needed for the second factor authentication: phone numbers for SMS messages, email addresses and Pledge identification details. All these details are stored under the user's personal database entry, the user account. As a context, this is the same kind of account that most of the office workers use every day to log in to their networked Windows computers.



In single factor authentications the users would log in to the Citrix Web Interface with their AD accounts and get access to XenApp applications right after that. When the second-factor authentication is implemented, the users have to first authenticate themselves with the AD account. After this they are directed to the second factor authentication. The second factor authentication can be pre-defined to one specific method, or then the user can choose from two or more alternative methods. In this test setup the user could choose to use SMS, email or software-based Pledge client.

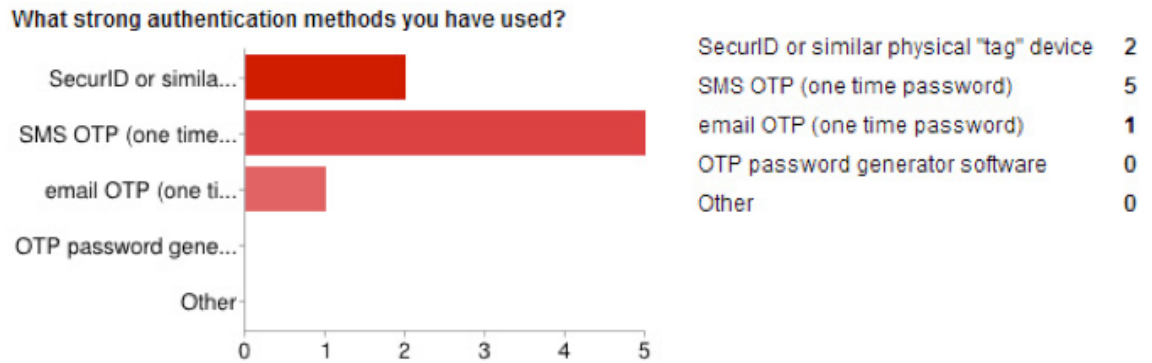
## 6 Results



This chapter will present the progress and results of the empirical study. The study, constructed in the previous chapter, was performed in January 2013 in the Helsinki metropolitan area, Finland. The test participants (n=6) were 23 – 27 years old students doing their Master studies in Aalto University. The more detailed demographic information is presented in section 6.1. Sections 6.2 – 6.5 will present the usability and security data gathered during the study. Then section 6.6 will present the qualitative data that was gathered during the study but did not fit the predefined metrics.

## 6.1 Demographics

The demographics of the conducted study reflect the planned user selection. Six people were interviewed for the study, half of them male and half of them female. The average age of participants was 25 years and they all reported having two or three years of work experience. They were either finalizing their master degree or graduated during the past year. The study background of the participants varied a lot, self-reported backgrounds were: Information and Service Management, Structural Engineering, Industrial Design, Information Networks, UX & Concept Designer, and Product Development.



*Figure 14. Strong authentication methods used by participants.*

---

In the freeform part of the pre-questionnaire, most of the people commented the SMS OTP to be the most usable and most secure solution they had used before the study. Five out of six participants reported having previous experience with strong authentication methods; all five had used SMS OTP, two had used a SecurID –device and one had used email OTP. One of the test participants reported having no previous experience with any strong authentication method, when “strong authentication method” was defined in the questionnaire to be anything more than username and password. In addition to the predefined answers (Figure 14), the questionnaire had a freeform field “other”, but no other authentication methods were listed. This might be a small fault in a test setup as the questions were leading towards separate technological solutions. Some of the participants later mentioned their Internet banking accounts and related authentication method, the cardboard password list typical to all major Finnish banks, as a strong authentication method. It is highly probable that all study participants use Internet banking regularly (Tilastokeskus, 2011) even though it was not mentioned by anyone in this stage of the pre-questionnaire.

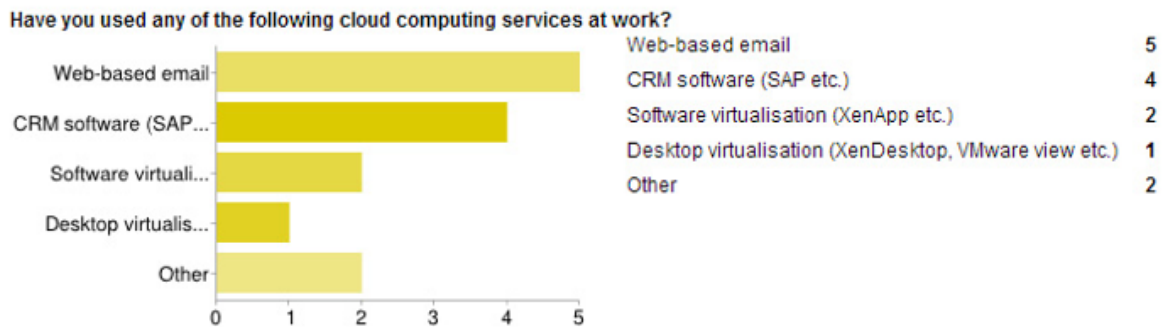


Figure 15. Cloud services used by the participants.

All of the test participants had at least some experience on cloud services (Figure 15). In addition to the predefined answers, users also mentioned two other services: Dropbox and project file management (the user did not remember the exact name of the service). The previous experiences of the users were mostly focused on the “light” SaaS solutions like webmail (100%) and CRM (67%). “When working correctly, virtualization is really good tool. On the other hand, single-function web-based tools that need separate logins tend to be less usable, especially because each of them usually having separate authentication.”, says one of the participants.

Only half of the users had some experience or knowledge about DaaS services (Figure 16), which was taken into account while going through the test scenario. The depth of the explaining the scenario was adjusted to match the perceived knowledge level of the individual user.

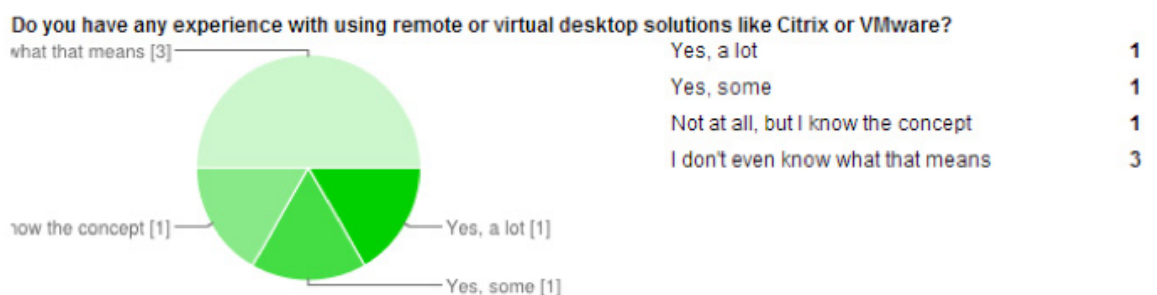


Figure 16. Participant experience with desktop virtualization.

## 6.2 Usability – Efficiency

Timing the login process in two parts was used to measure method efficiency as a part of usability. The order of these three second factor authentication methods was randomized, but all of the methods shared the identical first-factor authentication. The first part of the timing was the first factor login the users made with their self-generated accounts, consisting of an email address and a password. As assumed, this shows a noticeable improvement as the users repeated the login process, improving from 17,75 seconds average on the first login to 14,27 seconds average on the third login. The average login times and their standard deviations are presented in Table 2.

*Table 2. Average login times with the first-factor authentication.*

	<b>First Login</b>	<b>Second Login</b>	<b>Third Login</b>
<b>Average Login Time (s)</b>	17,75	14,87	14,27
<b>Average Login Time (s)</b>	0,93	1,32	1,37

After completing the first-factor authentication the participants continued straight to the second-factor authentication, choosing the testing method according to the random pre-selection. This part was timed separately; the results can be seen in Table 3.

As assumed, SMS was the fastest method as it does not require any additional authentication to see the code, like logging into the email account, and it requires less action steps than generating an OTP code with Pledge client.

On the email OTP, there was no significant difference between the authentication times even though the participants were told that they could read their emails any way they wanted. They used three different devices for reading the OTP emails: three of the six participants logged in with the test PC, two of the participants used their own smartphones and one of the participants used her own laptop she had with her. All of the users who used their personal devices had the auto-login feature enabled on their personal devices and they stated that it felt more comfortable than logging in on a new device would have felt.

There was no relevant variance with age or educational background that would have affected the results, as participants were quite homogenous in those aspects. Previous experience with

the authentication methods and overall work experience with computer systems seemed to have a positive effect on shortening the authentication times, but the test setup and amount of participants does not allow for a statistically significant analysis on these factors.

*Table 3. Average login times with second-factor authentication.*

	<b>SMS</b>	<b>Email</b>	<b>Pledge</b>
<b>Average Login Time (s)</b>	25,02	40,23	34,33
<b>Average Login Time (s)</b>	4,40	2,52	4,72

### 6.3 Usability – Effectiveness

All participants were able to complete the login and secondary authentication without any major issues. None of the participants needed instructions how to process the code or where to retrieve it.

One participant was having her first experience with SMS-based authentication and was looking at the blank field titled “One Time Password:”. She was about to ask “Should I have another password for this or...”, when her question was interrupted by the SMS notification. This immediately guided her to retrieve the code without finishing the original question.

Another participant was testing the Pledge and he was given a test phone with pre-installed client software. After completing the first-factor login, he just looks at the phone and does not start the software. After waiting for a while, he is prompted by the supervisor to start the software and he is able to complete the authentication without any further issues. According to his own description of the event, he was waiting the Pledge client to provide a similar push notification of the OTP code than the two earlier methods, SMS and email had.

Both of the issues were, in high probability, one-time errors. In the debriefing interview both of the users recognized the error situation and were able to fully and correctly analyze what went wrong, so it should be safe to assume that they were able to learn from the errors to prevent them easily in the future.

## 6.4 Usability – Satisfaction

The satisfaction element of usability was measured with a seven-step Likert questionnaire described in section 5.5. The results of the 18 questions presented to participants (Appendix A) are presented in Table 4. The mean usability scores (Table 5) were further derived from these answers.

SMS was evaluated with positive attitudes (over 5 on the Likert scale) on 8 of the 18 attributes (44,4%). The lowest result came from the need for improvement, but this attribute was consistently low on each of the tested methods, as all of the participants had some ideas for improving the methods. The second lowest attribute was the sense of security, which was still better than with email but considerably worse than with Pledge. On the positive side SMS was praised for its simplicity and speed of use.

Email got the least amount of positive attitudes from the tested methods, 7 out of 18 (38,9%) and it had also three borderline-negative attributes: the lack of trust, most need for improvement and least likable for using the method again. On the positive side email was seen as convenient and easy to use solution that did not need any instructions.

Pledge got the most positive attitudes, 9 out of 18 (50%) and it had only one attitude that was significantly worse compared to the other methods: knowing what to do next. It was also able to get just barely the best score in the need for improvement, but the received 3.67 (out of 7) clearly indicate that the participants thought that this method would still need improving. On the positive side, Pledge excelled on degree on trust, reliability and getting clearly the highest score in the question whether the participants would use the method again.



Table 4. Average login times with second-factor authentication.

	<b>SMS</b>	<b>Email</b>	<b>Pledge</b>
<b>Degree of trust</b>	4,83	3,83	5,33
<b>Stress</b>	4,83	4	4,5
<b>Method too complicated</b>	5	4	4,33
<b>Degree of control</b>	5,17	4,5	5
<b>Knew what to do next</b>	5,17	5,17	3,5
<b>Matching expectations</b>	4,33	5,33	4
<b>Would use the method again</b>	4,5	3,83	5,67
<b>I felt this method was reliable</b>	5	4,33	5,5
<b>Frustration</b>	5,33	4,67	4,83
<b>Speed of use</b>	6,17	4,67	5,67
<b>Improvement needed</b>	3,5	2,83	3,67
<b>User-friendliness</b>	4,83	5	5
<b>Degree of enjoyment</b>	4,67	4,5	4,33
<b>Degree of security</b>	4,17	4	5,33
<b>Need for instructions</b>	4,83	5	4
<b>Degree of convenience</b>	5	5,17	5,33
<b>Concentration</b>	4,67	5,17	4,5
<b>Ease generating code</b>	6,33	6	5

Overall the methods were really even in the evaluation. There were no clear peak attributes inside any of the methods. The overall score between the methods was also quite even, as the difference between the best and the worst mean usability rating was only 0,35 on a scale of 7 (Table 5).

*Table 5. Mean usability results from the methods*

	<b>SMS</b>	<b>Email</b>	<b>Pledge</b>
<b>Mean</b>	4,91	4,56	4,75
<b>Standard Deviation</b>	2,67	3,04	2,97
<b>N</b>	6	6	6

## 6.5 Comparative rating

The participants rated their overall preference (quality) of the three compared methods on a 30 cm scale as described in the section 5.5. They also evaluated separately the security and convenience of the methods on the same scale. As the users were encouraged to change the rating after testing each method if they felt it was necessary, the ranking score represents their opinion of the ranking of these factors. The mean ratings are shown in Table 6.

*Table 6. Comparative ratings between the authentication methods*

	<b>SMS</b>	<b>Email</b>	<b>Pledge</b>
<b>Convenience</b>	19,58	17,58	18,25
<b>Security</b>	18	12,92	20,75
<b>Quality (overall)</b>	20,75	15,83	21,75

In the overall comparison the Pledge was a winner with 1 point difference to SMS. Email was the least preferred solution, losing to Pledge with almost 6 points. From the individual factors, email lost to both SMS and Pledge by almost 5 and 8 points, while the difference between SMS and winning Pledge was 2,75 points. The third evaluation factor, convenience, saw the most even distribution of the three; all the methods were inside a 2-point distribution. Convenience was also the only factor that Pledge lost to SMS, with 1,25 points difference.

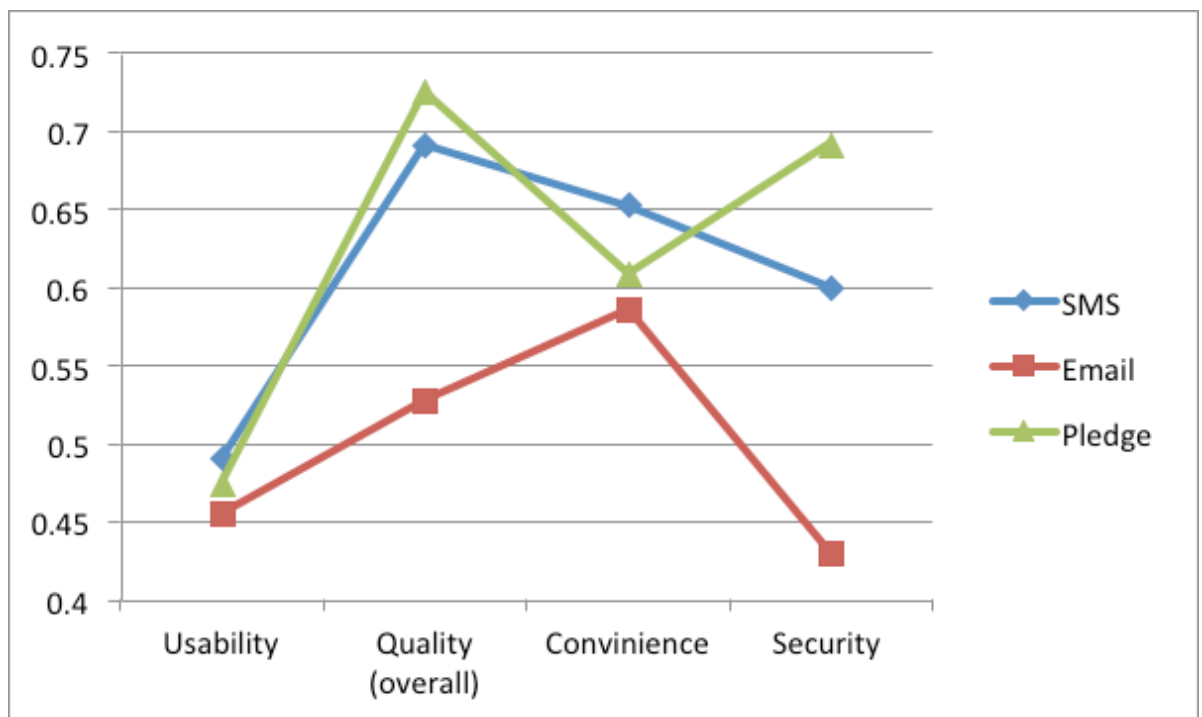


Figure 17. Usability, quality, convenience and security of the methods scores, maximum scores scaled to one.

To visualize all the measurement attributes (convenience, security, quality and mean usability), the individual attribute scores were scaled to a table, where the top score of one represents the maximum value for each category. The results are presented in Figure 17.

## 6.6 User insights

During the usability testing and the following debriefing interview, the participants had many comments on their perception of the tested authentication methods. Some of the responses are presented below, with the quotes taken from the participant comments made during the user testing and the debriefing interviews. Only two of the six interviews were in English; for the rest of the interviews the quotes are translated from Finnish with an effort to preserve the content as close to the original comments as possible. All participant comments can be found from the Appendix B.

### 6.6.1 SMS OTP

Many of the participants commented that SMS messages and their phone overall feels very personal and they felt this to have a direct connection to the security as well, especially compared to a lot less personal email. Having the phone always physically with you adds to the security, as one participant commented: “The phone feels a lot more secure and personal. Of course the losing and breaking are possible issues, but you don’t really think it would happen to you”. One of the participants had recent bad experiences about losing several phones in rapid succession, and as a result she admitted being more cautious about the security of SMS OTP: “I lose my phone quite often so security would really worry me”.

Another issue with SMS OTP was the required connection to the mobile network. Few of the participants have had trouble recently with their mobile reception in their office building, especially in the underground levels. The really remote locations with critical work tasks were also potentially really serious issues: “How would this work in critical situations at a difficult location like a remote windmill park? The backup methods and handling problems should be really smooth and efficient”. Having a backup method for SMS felt really im-

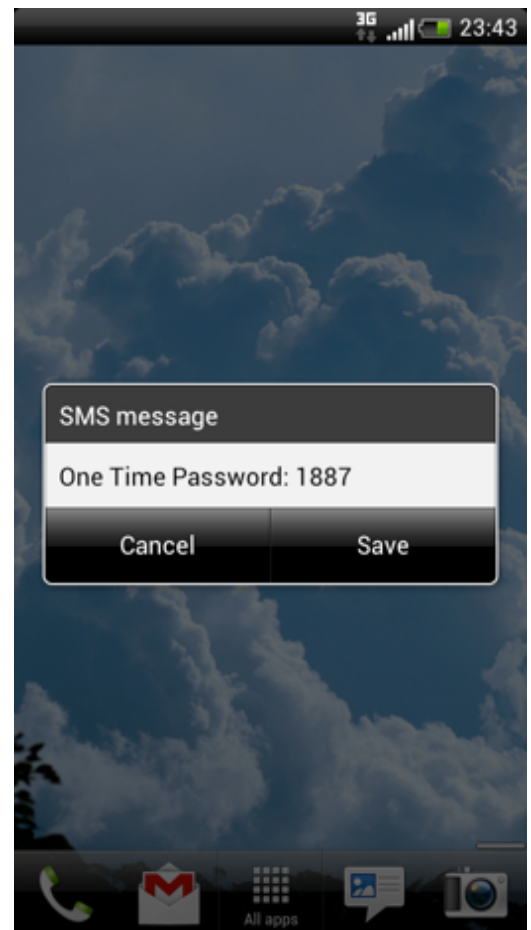


Figure 18. SMS OTP on an Android mobile phone

portant for many users, even for some of those users who preferred the method as an overall solution.

Code length and complexity was also mentioned; the participants appreciated the current code formatting (4 numbers) and told that it would be a lot less convenient if the code length or complexity would increase: “The length of the code has a big effect on convenience, 6 characters would be a lot less convenient than 4 characters in SMS, really stretching the work memory”. They felt that the added complexity would not really add security, as the code is valid only for a short period of time and is good only for a single use.

## 6.6.2 Email OTP

Email was praised for its convenience. Most of the participants used automatic login for email on their smartphones and laptops. This made the email to have good reviews on the convenience comparison. However, most participants also commented on the flipside of the convenience: “Email feels a lot less secure as it’s always open, it can be hacked and you’ll get a lot of spam” – the comment sums up the opinions about the email OTP as a method. Spam, security breaches, hacking and the overall amount of daily email were the most common reasons people disliked email as an OTP method.

Some of the participants felt that they just did not want to receive any additional email for any reason and wanted to keep the authentication separate. In two cases the company webmail also used the same account details that would probably be used as a primary authentication method in the DaaS scenario, so using corporate email as a secondary authentication would not bring any real additional security.

Email was mentioned a few times as a possible backup for SMS or Pledge. The other two methods were generally preferred over email, but participants realized both methods were relying heavily

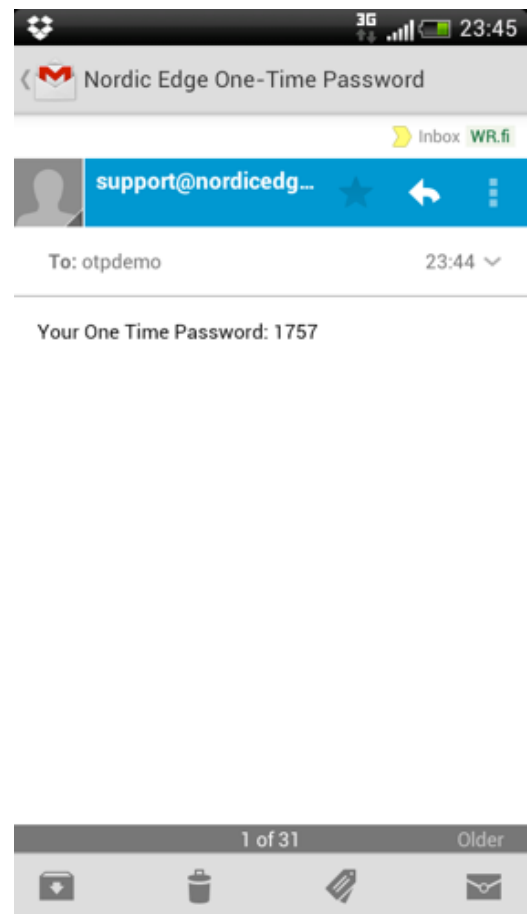


Figure 19. Email OTP message on an Android phone

on the functionality of the mobile network or their personal smartphone. “SMS feels the most usable solution and secure enough, but I would like to have email as a backup if e.g. my battery dies”.

In email OTP the opinions about the code length were divided; the people who preferred reading the emails with their smartphone (n=2) preferred shorter and simpler codes with the same reasoning than with SMS. However, most of the people who preferred to read the emails with the test PC (n =3) said that the code complexity does not really matter, as they can copy and paste it anyway from the email to the login window.

Reading emails and SMS messages on the smartphone revealed one additional security issue. Even though all the participants were using lockscreen passcodes, some of the smartphone models still revealed the received OTP code in the message preview without opening the phone. This could be avoided by instructing the users to disable message previews or modifying the OTP message body so, that the actual OTP code is not included in the previewed part of the message.

### 6.6.3 Pledge client

Pledge was the favorite authentication method for most of the users: “Pledge needs more effort but still feels more convenient than the other methods. The few extra clicks are really easy to learn and repeat with muscle memory without any thinking after that.” The participants also felt, that even though using Pledge was not the fastest way to authenticate for any of them, the interaction design of the software made it feel faster and more enjoyable to use: “Pledge felt quick even though it had more clicks, the software design like rolling numbers in the code generation helped that”. The McAfee brand was also recognized; almost all of the participants remembered that in the debriefing interview. Two of the participants stated that seeing a familiar and reliable brand like McAfee during the Pledge usage heightened their sense of security.

One participant commented that Pledge even felt more familiar way to authenticate than SMS and email, even though she reported having no experience with any strong authentication methods: ““This might be a bit old-fashioned way of think-

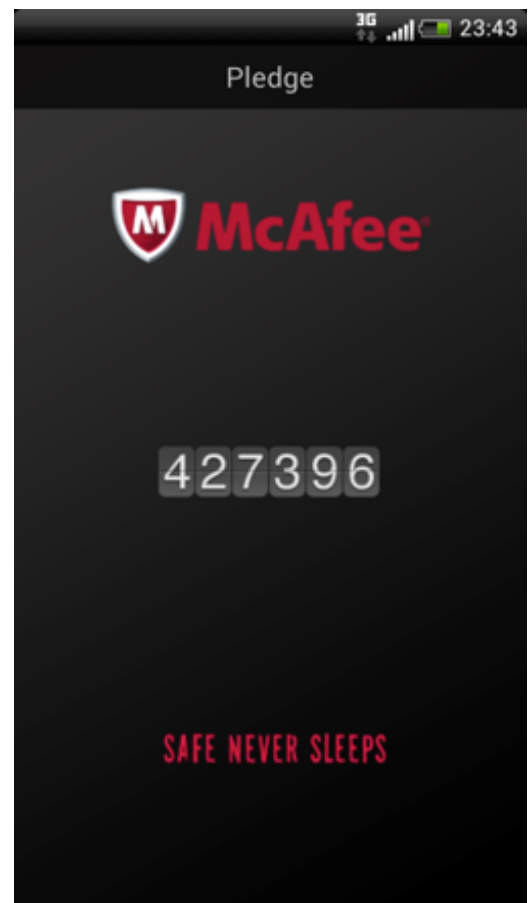


Figure 20. Pledge client on an Android phone

ing, but pledge feels almost like a paper version, like the cardboard badges you get from the bank”. Many participants also liked the fact that Pledge made it possible to keep the authentication separate from the already overflowing SMS and email inboxes. However, the participants were also worried about the possible issues with smartphone malfunctions or misplacing the phone altogether.

In the test scenario the pledge software came pre-installed “by your company’s IT-support”, and one participant stated that this is how it should be – he would not want to use his own phone or try to install the software himself: “Pledge client installations should be handled by the helpdesk. I would also definitely need a work phone for that; I wouldn’t want to use my own phone.”

#### **6.6.4 Strong authentication overall**

The users saw the need for strong authentication in the test scenario and had a positive attitude towards the idea of having a secondary authentication method in the login process: “Secondary authentication is really good, it adds to sense of security and sense of control”. They also saw the need for two-factor authentication outside the test scenario in their everyday computing: “Bank, personal information and internet shops would feel worth of two-factor authentication”.

The tested methods were appreciated and even though the competition between the three tested methods was tough, two of the participants clearly commented that they were better than the methods they are currently using: “Any of these methods feels a lot better than the paper password lists used with the Finnish banks”.

## 7 Conclusions and discussion



This chapter will present the results of the thesis research. Section 7.1 will summarize the thesis by answering to the research questions. Section 7.2 will discuss the overall validity and accuracy of the results. Section 7.3 will present the practical implementations of the thesis for designing business cloud authentication and section 7.4 will present ideas for future research.

## 7.1 Answering the research questions

**Rq1 Identify a) the common authentication methods used in business cloud authentication at the moment and b) emerging new authentication methods suitable for the purpose.**

The first aim of this thesis was to get a wide overview of the various authentication methods and strategies and reflect their validity in business cloud settings. This was achieved in chapter 4, which gives a detailed description of the identified methods and strategies.

Two major trends in business cloud authentication were identified: shared authentication and multi-factor authentication. Shared authentication aims to reduce the amount of user accounts needed on a daily basis by sharing the login details, for example Microsoft Active Directory account, to be used in multiple cloud services in addition to the workstation login. This improves authentication usability and in most cases also security, as the users do not have to cope with excess amount of user accounts (FIPS, 1985).

On the other hand, the cloud services are more open to the attacks because of their online connectivity. At the same time the security of the traditional combination of user ID and a password is eroding, as the increasing computational power makes it easier to crack the passwords with brute force and dictionary attacks (Honan, 2012). This has led to an increased adaptation of multi-factor authentication in business cloud services. Multi-factor authentication combines two or more authentication method categories for increased security: something you know, something you have, something you are or somebody you know.

At the moment almost all of the multi-factor authentication solutions for business cloud services are focusing on the categories “something you know” (e.g. a password) and “something you have” (e.g. a RSA tag). Implementing biometric authentication, “something you are”, in cloud authentication is currently challenging, as a secure biometric identification requires a scanner that can take accurate biometric measurements. In addition, a secure biometric authentication needs an environment that can guarantee that the biometric sample is provided in a legitimate manner, as the samples are easy to forge, for example by lifting a fingerprint from a drinking glass. In cases of stolen authentication information, a password is easy to reset. But

resetting the fingerprints of the user would cause severe pain and risk a permanent physical damage (Coventry, 2005). Both of these limitations of biometric authentication can be solved in a secure, fixed authentication environment, but that would negate most of the mobility- and multi-platform benefits of a cloud environment.

The fourth authentication category, somebody you know, is getting more attention in cloud authentication especially as a recovery option (Brainard et al., 2006). This method is still fairly unknown in the business context and it might encounter some psychological hindrances. Some people are considering an error in authentication, like forgetting a password, as a highly personal failure that they do not wish to share with their colleagues (Adams et al., 1999). This was confirmed by one of the empirical study participants, who strongly emphasized that he would never want to bother his coworkers with his authentication problems and admit forgetting a password if he could avoid it in any way.

The sensor capabilities of the mobile devices are improving all the time and some of these sensors can already be used for authentication. For example a facial authentication to unlock the device can be achieved easily by using the front-facing camera of a mobile phone. At the moment the resolution and capabilities of the mobile sensors are easy to bypass with a fake biometric input. But as the sensor accuracy improves and the sensors become ubiquitous enough, biometrics might become a valid authentication method in the business cloud.

Another emerging category in business cloud authentication is collaboration and authentication sharing with private cloud services. At the moment most corporate services rely on having a complete control of the user data and considering external, especially consumer-grade, user data as inherently untrustworthy. However, the customer-grade services like Facebook and Gmail are becoming more and more important for their users, and this is starting to reflect in their security and reliability as well. Especially Google has implemented many alternative authentication methods and multi-factor authentication. Combining this development with secure authentication sharing protocols like OpenID and OAuth, the commercial services might become at least one plausible factor in multi-factor authentication. This kind of development can already be seen with a Finnish internet banking authentication sharing system TUPAS, which is used for example to authenticate password resets in Aalto University (Aalto IT, 2013).

**Rq2 What are the most important factors, in addition to the authentication method itself, that are affecting the security – usability –balance of the entire authentication process and how they can be optimized for the business cloud authentication?**

The currently most popular authentication method, a combination of user ID and password, is being eroded by security concerns and more efficient cracking solutions, thus the more advanced and multi-factor solutions are gaining popularity. Excluding some forms of biometric authentication, the users will still forget their passwords, lose their SecurID tags or break their authenticating mobile phone, which leads to the need of resetting the authentication to a new password or to a new device (Bonneau, 2010). This also creates one possible attack vector that can destroy any of the authentication methods if the process is not designed properly. During the past year alone, attackers using the automatic password reset (Honan, 2012) and customer support (Cardinal, 2012) have accounted for many of the most damaging attacks against the legitimate users. There are several existing possibilities to counter this kinds of knowledge-based attacks, like requiring strong alternative authentication or physically authenticating the user before resetting the online authentication. One big emerging trend is also using the fourth authentication category, “somebody you know” (section 4.4) to support the online authentication resetting.

Another cornerstone of a successful authentication strategy is communicating with the users frequently about the security issues, helping them to select the most secure authentication methods and especially giving them the motivation to actually use the selected methods (Adams, 1999). No matter how advanced the technological solution is, users will be able to break it or bypass it if it is not aligned with their mindset and workflow (Renaud, 2012). In addition to adjusting the technical authentication to be as usable as possible, it is also important to adjust the psychological usability of the whole authentication process. It is essential to help the users to understand the reasoning for authentication in order for them to include it as a natural and functional part of their workflow.

**Rq3 How the usability and security aspects of authentication methods affect the user preference in method selection?**

When given a possibility to select from multiple authentication alternatives during the study, the study participants clearly put more emphasis on the security than usability or convenience, as seen in section 6.5. The overall usability scores of the three studied methods were really close to each other; the difference of the best and the worst method was only 0.35 points on a 7-point scale (5%). The security aspect of the methods had bigger variance in the test scores, 7.83 on a 30-point scale (26,1%) and the results correlated strongly with the user preference and evaluated overall method quality. Many of the test participants commented, that if the authentica-

tion is done daily or several times a day, as it was described in the test setup, even email OTP, the method with worst usability score of the tested methods, would be easy to learn after a few tries and repeat indefinitely after that. Like one of the test participants commented, “Pledge needs more effort but still feels more convenient than the other methods. The few extra clicks are really easy to learn and repeat with muscle memory without any thinking after that.”

Most of the test participants agreed, that they preferred security to usability in the scope of the three tested methods. However, during the debriefing interview some of the participants also mentioned that it is important that the usability has to be over a certain threshold, otherwise the security starts to lose importance. Defining such a threshold is highly subjective as it is affected by the many internal and external factors, as discussed in this thesis.

## 7.2 Validity and credibility of the study

The importance of usability has been recognized by the security- and authentication software makers (Whitten et al, 1999; NordicEdge 2013) and many improvements have been already made on that front during the recent years. Some of the previous research from the past decade (Weir et al., 2006, Whitten et al. 1999) shows a greater variance in usability evaluations and some of the previously tested solutions were not able to even pass the usability threshold of the test participants.

The goal of this thesis was to test a representative set of most popular current business cloud authentication methods, which was achieved. The tested methods were, however, quite homogenous and restricted to one authentication method category, “something you have”. The cloud context itself set quite many restrictions in selection of the tested authentication methods, as the authentication had to be independent of the used device and ubiquitous enough to be available for normal businesses.

With the current devices, having only a limited sensory and connectivity capabilities, the universal cloud authentication solutions can rely on only a limited set of input types. This excludes biometrics and most of the other device-based solutions like smartcards from the list of universal cloud authentication alternatives. And as biometrics has been one of the most varying subset from the usability-point-of-view (Coventry, 2005), this exclusion already limits the potential variance in the usability results of the cloud authentication. Some specific cloud services used in controlled environments, for example patient information systems in hospitals, can rely on to a more varying set of authentication methods as the accessing devices can be pre-defined.

The relatively small variance between the tested methods might be one explanation for the small (under 5%) variance for the usability score in section 6.4. However, as the overall results show a big variance between the tested four methods, and the method selection covered a large part of the currently used business cloud authentication solutions, it can be assumed that the method selection was wide enough for the selected scope.

The amount of participants in the study was relatively small and the group was homogenous in some, but not all, demographic criteria. The study gave a good description of the selected user category, under 30 year old students or professionals with academic education. However, as the business cloud authentication solutions are often implemented for the whole company, the results might not be directly applicable for all business environments. In many situations age, previous technical experience and level of education will affect the perceived usability and security of the solution (Lightner, 2003).

Users with significantly different demographics might prefer more familiar solutions like SMS, or the perceived usability of software-based solutions like Pledge mobile client might be lower. Still, the study showed that all of the authentication methods were easily adapted by novices, most of whom had no previous experience of such methods. Some users with less technical skills or experience might need a bit more guidance with the different methods or bit longer time to adapt to them.

## **7.3 Implementing the results in practice when designing business cloud authentication**

Multiple-factor authentication is more secure and more usable alternative than implementing traditional password-based authentication with extended password security requirements. In theory, requiring long, complicated and unique passwords that have to be changed frequently would increase the system security. However, in practice these requirements are often leading to reduced usability and users inventing workarounds against the system, leading to overall weaker security. Using multiple-factor authentication reduces the stress on one authentication method and adds security without compromising usability.

Business cloud services should have at least two-factor authentication. In some ultra-secure environments three-factor authentication or even specially designed biometrics authentication might bring additional security if the necessity of such authentication is communicated well to the users. However, if the reasoning for the strong authentication arrangement is not explained when the authentication is implemented, a big part of the security benefits is eroded as the users start to develop their workarounds.

In some situations, the False Rejection Rate (FRR, system not authenticating the authorized users) could become a very serious problem. For example when the employees are located or travel to foreign countries, SMS OTP messages might not be delivered properly. The authentication technology is generally planned for reliability and these kinds of glitches are rare, but they do happen. In addition, implementing an alternative second-factor authentication is usually very cost-efficient; most of the commonly used authentication software already contain the support for several authentication alternatives. Increasing the user alternatives also has the added benefit for optimizing the overall authentication usability, as the users can select their most preferred alternative instead of conforming to the single authentication method.

## 7.4 Ideas for future research

Restricted, precisely defined environments like hospitals and government offices are starting to implement a growing part of their daily tasks with cloud services that still require a heightened security and individual accountability. These would be really interesting environments to test the suitability of biometric authentication or “something you have” –type of authentication that is based on restricted authentication technology already used in such premises. One interesting example of this kind of solutions would have been Finnish Toimikortti, which is already widely used in the healthcare sector for various authentication solutions.

# References



Aalto IT, 2013. password.aalto.fi . [ONLINE] Available at: <https://password.aalto.fi/>. [Accessed 17 March 2013].

ABRAN, A., KHELIFI, A., SURYN, W. and SEFFAH, A., 2003. Usability meanings and interpretations in ISO standards. *Software Quality Journal*, 11(4), pp. 325-338.

ADAMS, A. and SASSE, M.A., 1999. Users are not the enemy. *Communications of the ACM*, 42(12), pp. 40-46.

ANCHAN, D. and PEGAH, M., 2003. Regaining single sign-on taming the beast, *Proceedings of the 31st annual ACM SIGUCCS fall conference 2003*, ACM, pp. 166-171.

ARMBRUST, M., FOX, A., GRIFFITH, R., JOSEPH, A.D., KATZ, R., KONWINSKI, A., LEE, G., PATTERSON, D., RABKIN, A. and STOICA, I., 2010. A view of cloud computing. *Communications of the ACM*, 53(4), pp. 50-58.

BEATY, K., KOCHUT, A. and SHAIKH, H., 2009. Desktop to cloud transformation planning, *Parallel & Distributed Processing, 2009. IPDPS 2009. IEEE International Symposium on 2009*, IEEE, pp. 1-8.

BestBuy, 2013. Password Help [ONLINE] Available at: <http://www.bestbuy.com/site/Using-My-Account/Password-Help/pcmcat204400050052.c?id=pcmcat204400050052> [Accessed 17 March 2013].

BISHOP, M., 2005. Realigning Usability and Security. *Security and usability*, , pp. 103-128.

BLEZARD, D.J. and MARCEAU, J., 2002. One user, one password: integrating unix accounts and active directory, *Proceedings of the 30th annual ACM SIGUCCS conference on User services 2002*, ACM, pp. 5-8.

BONNEAU, J. and PREIBUSCH, S., 2010. The password thicket: technical and market failures in human authentication on the web, *Proc. WEIS 2010*.

BRAINARD, J., JUELS, A., RIVEST, R.L., SZYDLO, M. and YUNG, M., 2006. Fourth-factor authentication: somebody you know, *Conference on Computer and Communications Security: Proceedings of the 13 th ACM conference on Computer and communications security 2006*, pp. 168-178.

BREAUGH, J.A. and FARABEE, A.M., 2012. Telecommuting and Flexible Work Hours: Alternative Work Arrangements that Can Improve the Quality of Work Life. *Work and Quality of Life*, , pp. 251-274.



BURT, J., 2011. BYOD trend pressures corporate networks. *eWeek*, 28(14), pp. 30-31.

BUYYA, R., YEO, C.S., VENUGOPAL, S., BROBERG, J. and BRANDIC, I., 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6), pp. 599-616.

Cardinal, 2012. Two-for-one: Amazon.com's Socially Engineered Replacement Order Scam :: HTMLList.com, A Web Development Blog by Synapse Studios. [ONLINE] Available at: <http://www.htmlist.com/rants/two-for-one-amazon-coms-socially-engineered-replacement-order-scam/>. [Accessed 17 March 2013].

Citrix, 2013. Citrix eDocs [ONLINE] Available at: <http://support.citrix.com/proddocs>. [Accessed 17 March 2013]

COHEN, F., 1997. Information system defences: A preliminary classification scheme. *Computers & Security*, 16(2), pp. 94-114.

COLMAN, A.M., 2006. Oxford reference online: A dictionary of psychology. Oxford University Press.

COSKUN, B. and HERLEY, C., 2008. Can "Something You Know" Be Saved? *Information Security*, , pp. 421-440.

COVENTRY, L., 2005. Usable biometrics. *Designing Secure Systems that People Can Use*. O'Reilly, , pp. 175-198.

CRANOR, L. and GARFINKEL, S., 2005. Security and usability: designing secure systems that people can use. O'Reilly Media, Incorporated.

DE ALVARÉ, A.M., 1988. How crackers crack passwords or what passwords to avoid, .

DE ALVARE, A. and SCHULTZ JR, E., 1988. A framework for password selection.[Password recommendations], .

EMC, 2013. Information Security - Governance Risk and Compliance - RSA - EMC. [ONLINE] Available at: <http://www.emc.com/security/index.htm>. [Accessed 17 March 2013].

FIPS 112 - Password Usage.1985. FIPS 112 - Password Usage. [ONLINE] Available at: <http://www.itl.nist.gov/fipspubs/fip112.htm>. [Accessed 23 September 2012].

GRANGER, S., 2001. Social engineering fundamentals, part I: hacker tactics. *Security Focus*, December, 18.

- GUNSON, N., MARSHALL, D., MCINNES, F. and JACK, M., 2011. Usability evaluation of voiceprint authentication in automated telephone banking: Sentences versus digits. *Interacting with Computers*, 23(1), pp. 57-69.
- HASSENZAHL, M. and TRACTINSKY, N., 2006. User experience-a research agenda. *Behaviour & Information Technology*, 25(2), pp. 91-97.
- HERLEY, C. and VAN OORSCHOT, P., 2012. A research agenda acknowledging the persistence of passwords. *Security & Privacy, IEEE*, 10(1), pp. 28-36.
- Honan, M., 2012. Kill the Password: Why a String of Characters Can't Protect Us Anymore [ONLINE] Available at: <http://www.wired.com/gadgetlab/2012/11/ff-mat-honan-password-hacker/>. [Accessed 18 November 2012].
- IBM, 2008. SOA, ESB and Beyond. [ONLINE] Available at: [https://www.ibm.com/developerworks/mydeveloperworks/blogs/sbose/entry/gathering\\_clouds\\_of\\_xaas?lang=en](https://www.ibm.com/developerworks/mydeveloperworks/blogs/sbose/entry/gathering_clouds_of_xaas?lang=en) [Accessed 17 March 2013].
- IETF, 2006. Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map [ONLINE] Available at: <https://tools.ietf.org/html/rfc4510> [Accessed 17 March 2013].
- ISO, W., 1998. 9241-11. Ergonomic requirements for office work with visual display terminals (VDTs). The international organization for standardization, .
- ITU-T STUDY GROUP, International Telecommunication Union, The International Public Telecommunication Numbering Plan, E. 164. Series E: Overall Network Operation, 19970501.
- JTC, I. and SC27, I., 2005. IEC 27002: 2005. Information technology-Security techniques-Code of practice for information security management, .
- KAILA, P., 2008. OAuth and OpenID 2.0. From End-to-End to Trust-to-Trust, , pp. 18.
- KAMP, P., GODEFROID, P., LEVIN, M.Y., MOLNAR, D., MCKENZIE, P., STAPLETON-GRAY, R., WOODCOCK, B. and NEVILLE-NEIL, G.V., 2012. LinkedIn Password Leak: Salt Their Hide. *Queue*, 10(6), pp. 20.
- KLINE, P., 1999. *Handbook of psychological testing*. Routledge.
- KO, M.N., CHEEK, G.P., SHEHAB, M. and SANDHU, R., 2010. Social-networks connect services. *Computer*, 43(8), pp. 37-43.
- LIKERT, R., 1932. A technique for the measurement of attitudes. *Archives of psychology*, .

MALTONI, D., MAIO, D., JAIN, A.K. and PRABHAKAR, S., 2009. Handbook of fingerprint recognition. Springer.

Market-Visio, 2013. Pilvipalvelujen hyödyntäminen 2013 [ONLINE] Available at <http://www.marketvisio.fi/fi/tutkimukset/it-palvelut/1611-pilvipalvelujen-hyodyntaminen-2013-loppukayttajatutkimus> [Accessed 17 March 2013].

MARSTON, S., LI, Z., BANDYOPADHYAY, S., ZHANG, J. and GHALSASI, A., 2011. Cloud computing—The business perspective. *Decision Support Systems*, 51(1), pp. 176-189.

MATYAS JR, V. and RIHA, Z., 2003. Toward reliable user authentication through biometrics.

*IEEE Security & Privacy*, 1(3), pp. 45-49.

McKendrick. 2012. NIST definition of cloud computing doesn't go far enough | ZDNet. [ONLINE] Available at: <http://www.zdnet.com/blog/service-oriented/nist-definition-of-cloud-computing-doesnt-go-far-enough/8634>. [Accessed 23 September 2012].

MELL, P. and GRANCE, T., 2011. The NIST definition of cloud computing (draft). NIST special publication, 800, pp. 145.

NANCY, J.L., 2003. What users want in e-commerce design: effects of age, education and income. *Ergonomics*, 46(1-3), pp. 153-168.

NIELSEN, J. and HACKOS, J.A.T., 1993. Usability engineering. Academic press San Diego.

NordicEdge, 2013. Nordic Edge live authentication demo [ONLINE] Available at: <http://demo.nordicedge.com/about> [Accessed 18 January 2013].

NORMAN, D.A., 2009. THE WAY I SEE IT When security gets in the way. *interactions*, 16(6), pp. 60-63.

ORCHO, 2008. File:SecureID token new.JPG - Wikipedia, the free encyclopedia. [ONLINE] Available at: [http://en.wikipedia.org/wiki/File:SecureID\\_token\\_new.JPG](http://en.wikipedia.org/wiki/File:SecureID_token_new.JPG). [Accessed 17 March 2013].

PALLIS, G., 2010. Cloud computing: The new frontier of internet computing. *Internet Computing, IEEE*, 14(5), pp. 70-73.

REID, B., 1991. Reflections on some recent widespread computer break-ins, Computers under attack: intruders, worms, and viruses 1991, ACM, pp. 145-149.

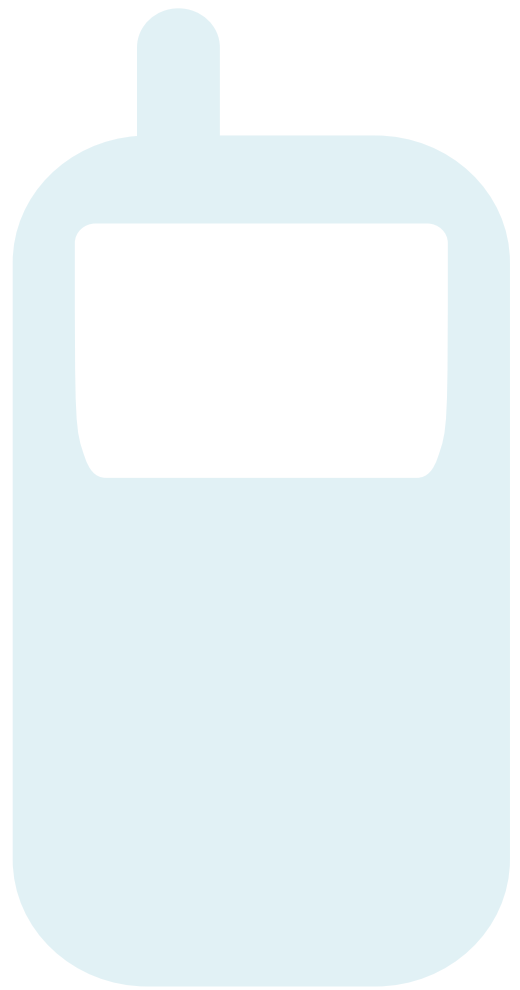
RENAUD, K., 2012. Blaming Noncompliance Is Too Convenient: What Really Causes Information Breaches? *Security & Privacy, IEEE*, 10(3), pp. 57-63.

RENAUD, K., 2005. Evaluating authentication mechanisms. *Security and usability*, , pp. 103-128.

- RISSANEN, T., 2010. Electronic identity in Finland: ID cards vs. bank IDs. *Identity in the Information Society*, 3(1), pp. 175-194.
- ROOT, R.W. and DRAPER, S., 1983. Questionnaires as a software evaluation tool, *Proceedings of the SIGCHI conference on Human Factors in Computing Systems 1983*, ACM, pp. 83-87.
- ROSS, B., JACKSON, C., MIYAKE, N., BONEH, D. and MITCHELL, J.C., 2005. Stronger password authentication using browser extensions, *Proceedings of the 14th Usenix Security Symposium 2005*.
- SALTZER, J.H. and SCHROEDER, M.D., 1975. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9), pp. 1278-1308.
- SASSE, M.A., BROSTOFF, S. and WEIRICH, D., 2001. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal*, 19(3), pp. 122-131.
- SHNEIDERMAN, B. and PLAISANT, C., 2004. *Designing the user interface, strategies for effective human-computer interaction (international edition)*, ).
- SHNEIDERMAN, B. and PLAISANT, C., 2004. *Designing the user interface, strategies for effective human-computer interaction (international edition)*, ).
- SplashData, 2012. Scary Logins: Worst Passwords of 2012 — and How to Fix Them. [ONLINE] Available at: <http://splashdata.com/press/PR121023.htm>. [Accessed 17 March 2013].
- SRIPANIDKULCHAI, K. and SUJICHANTARARAT, S., 2012. A business-driven framework for evaluating cloud computing, *Network Operations and Management Symposium (NOMS), 2012 IEEE 2012*, IEEE, pp. 1335-1342.
- SUBASHINI, S. and KAVITHA, V., 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), pp. 1-11.
- Tilastokeskus, 2011. Tilastokeskus - Suomalaiset käyttävät aktiivisesti sähköisiä viranomaispalveluja. [ONLINE] Available at: [http://www.tilastokeskus.fi/artikkelit/2011/art\\_2011-12-12\\_006.html?s=0](http://www.tilastokeskus.fi/artikkelit/2011/art_2011-12-12_006.html?s=0). [Accessed 17 March 2013].
- TREWIN, S., SWART, C., KOVED, L., MARTINO, J., SINGH, K. and BEN-DAVID, S., 2012. Biometric authentication on a mobile device: a study of user effort, error and task disruption, *Proceedings of the 28th Annual Computer Security Applications Conference 2012*, ACM, pp. 159-168.
- WEAVER, A.C., 2006. Biometric authentication. *Computer*, 39(2), pp. 96-97.

- WEIR, C., MCKAY, I. and JACK, M., 2007. Functionality and usability in design for eStatements in eBanking services. *Interacting with Computers*, 19(2), pp. 241-256.
- WEIR, C.S., ANDERSON, J.N. and JACK, M.A., 2006. On the role of metaphor and language in design of third party payments in eBanking: Usability and quality. *International Journal of Human-Computer Studies*, 64(8), pp. 770-784.
- WEIR, C.S., DOUGLAS, G., CARRUTHERS, M. and JACK, M., 2009. User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security*, 28(1), pp. 47-62.
- WEIR, C.S., DOUGLAS, G., CARRUTHERS, M. and JACK, M., 2009. User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security*, 28(1), pp. 47-62.
- WHITTEN, A. and TYGAR, J.D., 1999. Why Johnny can't encrypt: A usability evaluation of PGP 5.0, *Proceedings of the 8th USENIX Security Symposium 1999*.
- WIXON, D. and WILSON, C., 1997. The usability engineering framework for product design and evaluation. *Handbook of human-computer interaction*, 2, pp. 653-668.
- Yung, 2011. An Inconvenient Truth of the NIST Definition of Cloud Computing, SP 800-145 [ONLINE] Available at: <http://blogs.technet.com/b/yungchou/archive/2011/12/19/an-inconvenient-truth-of-the-nist-definition-of-cloud-computing-sp-800-145.aspx> [Accessed 17 March 2013].

# Appendices



## Appendix A : Usability of security in Likert scale

Based on Weir et al., 2006, 2007, 2009; Cranor et al. 2005, Likert 1932

To balance the positive and negative responses, half of the questions were inverted to a negative setting. These are listed below with (INV) –tag.

1. I found this method trustworthy
2. I felt under stress while using the method (INV)
3. Using this method was too complicated (INV)
4. I felt in control when using this method
5. When using this method I didn't always know what to do next (INV)
6. This method did not match my expectations (INV)
7. I would be happy to use this method again
8. I felt this method was reliable
9. Using the method was very frustrating (INV)
10. Using this method was quick
11. I feel that this method needs a lot of improvement (INV)
12. I found this method 'user-friendly'
13. I did not enjoy using this method (INV)
14. Using this method felt secure
15. I needed instructions to use this method (INV)
16. I thought this method was convenient
17. I had to concentrate hard to use the method (INV)
18. Knowing how to generate the code was easy.

## Appendix B : Participant comments from the debriefing interview

### Participant 1 (27 years old, female, Information and Service Management)

All the methods were quite convenient.

SMS and email were more familiar, so they seemed more convenient. Pledge was new, but it would probably be as convenient.

Laptop logs automatically to email, so it feels like a more insecure alternative

Phone is usually with her and feels more secure than laptop that might be out of sight longer. Phone feels more personal than a computer, so it feels more secure as well

Secondary authentication is really good, it adds to sense of security and sense of control. In reality it might not be more secure in the end, because your computer or phone is usually just lying around.

Really liked that the OTP code included only numbers. From email it is easy to copy paste, but writing long codes with big and small letters, numbers and “something really random”

It’s already secondary authentication, so the complexity of the code doesn’t really seem relevant.

It’s ok to see the OTP code when writing it to the website, as it is just for one use. Hiding it would add difficulty to the writing, but would not create any additional security

### Participant 2 (27 years old, male, Structural Engineering)

Could the pre-existing bank authentication used for this as well? Or at least as a backup if the user can’t use the primary method.

Pledge client installations should be handled by the helpdesk. I would also definitely need a work phone for that; I wouldn’t want to use my own phone.

Using colleagues as a backup authentication (“somebody you know”) might work, but it would need a lot of practice. Usually people don’t want to admit their mistakes.



How would these work in a critical situations at a difficult location like a remote windmill park? The backup methods and handling problems should be really smooth and efficient.

I would like to do the strong authentication only once per workday, it should be enough.

What if I have problems with my smartphone and have to use my backup phone

Pledge would be great: Less SMS (I get too much of them already) and it works with a bad reception

Our webmail has the same login details than our desktop (Windows AD) - the email as a second factor would not work with this setup.

The need for extra logins and the distribution of needed knowledge between several different systems is sometimes annoying.

I've got a folder called "account details" ("tunnistautuminen") in my email. It has all the randomly used work accounts that I would otherwise forget. Nobody is probably interested with the content, as they are only tools, standard libraries etc., and stuff that people can access a lot easier in other ways than stealing my accounts.

It would be really helpful to have some consulting and teaching the basic principles like memory rules at work, especially for workers that are not that experienced with technology.

I'm creating my own password with a memory rule: a basic part + context part (from the service name) + the changing part. The changing part changes regularly and I can usually get in at least after trying 2 or 3 changing parts around the account creation time.

### **Participant 3 (24 years old, female, Industrial Design)**

Strong authentication was easy to use; I didn't have any big problems

Email felt like the most difficult solution because of the extra effort needed for the login. However, it would be a lot easier if I had been using auto login on my own PC

Pledge would be the best solution, as it doesn't burden the other messaging channels. I would like to keep authentication separate from my own emails and SMS

Pledge, being an offline service, feels a lot more reliable than especially email. Spam and possible security breaches reduce the position of the email a lot.

Pledge feels a lot more like the cardboard badges you get from the bank.

“This might be a bit old-fashioned way of thinking, but pledge feels almost like a paper version, compared to SMS and email”

### **Participant 4 (23 years old, male, Information Networks)**

“Wow, a pop-up message” - SMS arriving as a special message (off-inbox popup) was technically impressing for the test subject.

Email is open all the time, so it's clearly the most usable

Email feels a lot less secure as it's always open, it can be hacked and you'll get a lot of spam.

The phone feels a lot more secure and personal. Of course the losing and breaking are possible issues, but you don't really think it would happen to you.

The length of the code has a big effect on convenience, 6 characters were lot less convenient than 4 characters in SMS and email, really stretching the work memory.

In emails the OTP code complexity doesn't really matter, I'll just copy-paste it anyways

McAfee-brand brings some credibility to Pledge client, but not that much

If I would not care about security, I would choose email because of the convenience. However, I would really chose SMS because it was convenient enough and feels really secure

I wouldn't want to get any more emails than I already do.

### **Participant 5 (26 years old, female, UX & Concept Designer)**

SMS felt really convenient and easy, enjoyable to use

The SMS and email passcodes are visible on her iPhone without opening the screen lock -> feels like she's got less control about them. Plus a potential security threat.

I lose my phone quite often so security would really worry me

Pledge needs more effort but still feels more convenient than the other methods. The few extra clicks are really easy to learn and repeat with muscle memory without any thinking after that.

“I had fun with email, but didn't feel secure”

In my opinion, convenience needs both easiness (usability) and security

Pledge is the only one that gives me the full control, I can choose exactly when to generate the code

Pledge felt quick even though it had more clicks, the software design like rolling numbers in the code generation helped that

Pledge: “No typing, just tapping” - easy to control

It would feel more secure to visually delete the code after use and not to use the system back-button

McAfee-brand brought more feeling of security to the Pledge client.

## **Participant 6 (25 years old, male, Product Development)**

Now when I realized what it was, I have actually been using the SMS-based strong authentication before

SMS feels more personal and trustworthy than email  
Bank, personal information and internet shops would feel worth of two-factor authentication

Any of these methods feels a lot better than the paper password lists used with the Finnish banks

A big security company like McAfee or a familiar bank would bring a lot more credibility the solution

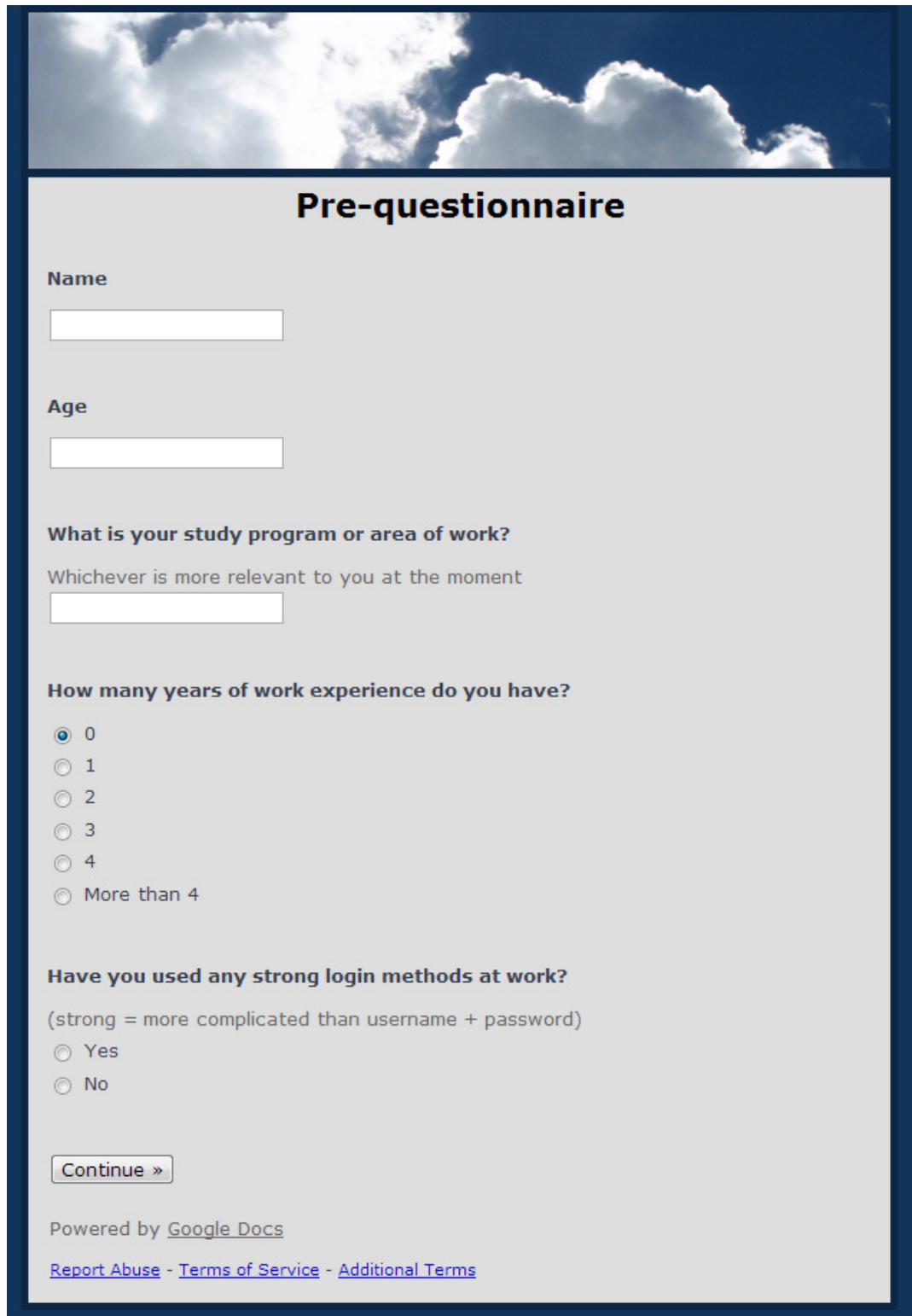
I wouldn't trust Google, Facebook or some other company that doesn't have its main focus on security

Using this solution with every login (to a virtual desktop) would feel like a burden, I would trust a long password to be secure enough

I would like to use a virtual desktop, and I would use the required strong authentication if there were no way to avoid using it

SMS feels the most usable solution and secure enough, but I would like to have email as a backup if e.g. my battery dies.

## Appendix C : Pre-questionnaire for the test participants



**Pre-questionnaire**

**Name**

**Age**

**What is your study program or area of work?**  
Whichever is more relevant to you at the moment

**How many years of work experience do you have?**

0  
 1  
 2  
 3  
 4  
 More than 4

**Have you used any strong login methods at work?**  
(strong = more complicated than username + password)

Yes  
 No

Powered by [Google Docs](#)

[Report Abuse](#) - [Terms of Service](#) - [Additional Terms](#)



## Pre-questionnaire

### What strong authentication methods you have used?

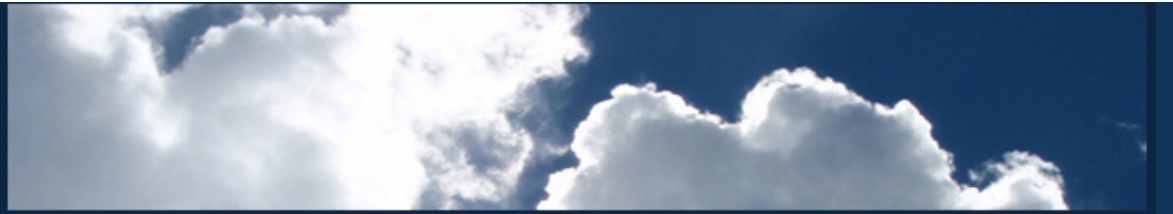
- SecurID or similar physical "tag" device
- SMS OTP (one time password)
- email OTP (one time password)
- OTP password generator software
- Other:

### Which was the easiest to use and why?

### Which one was the most secure and why?

Powered by [Google Docs](#)

[Report Abuse](#) - [Terms of Service](#) - [Additional Terms](#)



## Pre-questionnaire

**Have you used any of the following cloud computing services at work?**

- Web-based email
- CRM software (SAP etc.)
- Software virtualisation (XenApp etc.)
- Desktop virtualisation (XenDesktop, VMware view etc.)
- Other:

**Which was the easiest to use and why?**

**Which one did you think was the most secure and why?**

Powered by [Google Docs](#)

[Report Abuse](#) - [Terms of Service](#) - [Additional Terms](#)



## Pre-questionnaire

**Do you have any experience with using remote or virtual desktop solutions like Citrix or VMware?**

Also known as desktop virtualisation, desktop cloud or DaaS

- Yes, a lot
- Yes, some
- Not at all, but I know the concept
- I don't even know what that means

**If yes, what kind of?**

Powered by [Google Docs](#)

[Report Abuse](#) - [Terms of Service](#) - [Additional Terms](#)

## Appendix D : Likert questionnaire for the test participants



**Likert**

\* Required

**Name**

**Delivery method**

Mail  
 SMS  
 Pledge

**I found this method trustworthy \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree

**I felt under stress while using the method \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree

**Using this method was too complicated \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree

**I felt in control when using this method \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree

**When using this method I didn't always know what to do next \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree

**This method did not match my expectations \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree

**I would be happy to use this method again \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree

**I felt this method was reliable \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree



**Using the method was very frustrating \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree

**Using this method was quick \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree

**I feel that this method needs a lot of improvement \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree

**I found this method 'user-friendly' \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree

**I did not enjoy using this method \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree

**Using this method felt secure \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree

**I needed instructions to use this method \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree

**I thought this method was convenient \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree

**I had to concentrate hard to use the method \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree

**Knowing how to generate the code was easy. \***

1 2 3 4 5 6 7

Strongly disagree        Strongly agree

Powered by [Google Docs](#)

[Report Abuse](#) - [Terms of Service](#) - [Additional Terms](#)



