Risk analysis for Privacy and Identity Management

Gaute B. Wangen

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2012

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Risk analysis for Privacy and Identity Management

Gaute B. Wangen

01/07/2012

Abstract

The concept of privacy was recognized as early as the time of Aristotle [1], and has been a theme of debate since. Risks to privacy are problematic because the concept of "privacy" holds different meaning and importance to different people and cultures. What is considered private in Europe, may not be considered private in China, and vice versa. This makes defining and detecting risks to privacy a complex matter.
As people become increasingly dependent on online services, the amount of credentials that need to be remembered grows at the same pace. Identity management systems (IdMS) have been invented and implemented to, among other things, help users and organizations manage their electronic identities. Identity management (IdM) is found in all aspects of our electronic society, and many vendors are now offering IdMS to their customers. IdM is still a relatively new concept from a technology point of view, and the potential privacy invasions these systems pose are not well understood. Possibilities presented to attackers and targets in IdMS are many and complex, and the main objective of this research is therefore to better understand risks to privacy in IdMS using risk analysis.
In this project two case studies were conducted on a scenario based on the MinID IdMS [2] developed by Difi [3]. This project aims to help increase the knowledge regarding risks to privacy in identity management systems, and to use the stakeholder approach as a method for discovering privacy risks in identity management systems. The results from this thesis can be used by other risk assessment practitioners looking to conduct privacy risk assessments on IdMS. The two approaches used in this project was the Privacy Impact Assessment(PIA) [4] and the Risk IT framework [5].
The main conclusions of this project was:

- Risk IT is a more mature framework than PIA, but it requires prior knowledge of privacy risks to used for privacy risk assessment purposes. PIA is not easy to use and the practitioners have to choose their own tools for stakeholder and risk analysis, but it provides guidance for "privacy" and can therefore be used without prior knowledge of the subject.
- From a cost-benefit point of view, the Risk IT framework is the superior choice of approach compared to the Privacy Impact Assessment.
- PIA resulted in a larger number of risks with high diversity, but the process was not as cost-effective regarding work hours. Risk IT was cost effective and detected a large amount of privacy risks in a short period of time, but did not detect risks with the same diversity as PIA.
- The stakeholder analysis methodology used for privacy threat identification was successful in this thesis, but it needs more experimenting to verify validity.
- Privacy risks within 15 of the 19 privacy risk classifications by Solove [6] and PIA [4] was detected in the IdMS of this thesis.

Sammendrag

Begrepet personvern ble anerkjent så tidlig som i tiden til Aristoteles [1] og har vært et tema for debatt siden. Personvernsrisikoer er problematiske fordi begrepet "personvern" har forskjellig betydning for ulike mennesker og kulturer. Hva regnes som privat i Europa, anses ikke nødvendigvis som privat i Kina, og vice versa. Dette gjør at arbeidet med å definere og avdekke risikoer for personvernet en kompleks oppgave.
Ettersom folk blir stadig mer avhengige av nettbaserte tjenester, vokser mengden av legitimasjon som trenger å bli husket i samme tempo. Identitet styringssystemer (IdMS) har blitt oppfunnet og implementert for å blant annet hjelpe brukere og organisasjoner håndtere sine elektroniske identiteter. Identitetsstyring (IdM) er funnet i alle aspekter av vår elektroniske samfunn, og mange leverandører tilbyr nå IdMS til sine kunder. IdM er fortsatt en relativt ny teknologi sett fra et teknologiperspektiv. Det er en mangel på forståelse for de potensielle truslene som disse systemene utgjør for personvernet. Mulighetene presentert for angripere i identitet styringssystemer er mange og komplekse, og det viktigste målet med denne forskningen er derfor å oppnå en bedret forståelse risikoen til personvernet i IdMS. Den valgte tilnærming til dette problemet i denne avhandlingen er risikoanalyse.
Det ble utført to case-studier på et scenario basert på MinID [2], som er et IdMS utviklet av Difi [3]. Dette prosjektet har hatt som mål å bidra til å øke kunnskapen om personvernsrisikoer i identitet styringssystemer, og å bruke analyse av interessenter som en metode for å oppdage personvernstrusler i systemene. Resultatene fra denne oppgaven kan brukes av andre risikovurdering utøvere som ønsker å gjennomføre personlige risikovurderinger på IdMS. De to risikovurderingstilnærmingene brukt i denne oppgaven er Privacy Impact Assessment (PIA) [4] og Risk IT framework [5].
Følgende er et sammendrag av hovedkonklusjonene i dette prosjektet:

- Risk IT er et mer modent rammeverk enn PIA, men det krever forkunnskaper om personvernsrisikoer for å kunne brukes for risikovurderinger av personvern. PIA er ikke lett å bruke og utøverne må velge sine egne verktøy for interessentene og risikoanalyse, men den gir veiledning for "privatliv" og kan derfor brukes uten inneha kunnskap om emnet.
- Fra et kost-nytte-perspektiv så er Risk IT rammeverket det overlegne valget av tilnærming til analyse av personvernsrisikoer sammenlignet med PIA.
- PIA resulterte i et større antall risikoer med høyere mangfold, men prosessen var ikke så kostnadseffektivt på arbeidstid. Risk IT oppdaget en stor mengde personvernsrisikoer over en kortere tidsperiode og var svært kostnadseffektivt, men finner ikke personvernsrisikoer med det samme mangfoldet som PIA.
- Interessentanalysemetodikken brukt til å avdekke personvernstrusler viste seg å være velykket til dette formål i denne avhandlingen, men har behov for mer eksperimentering for å

verifisere gyldigheten.

- Det ble avdekket personvernsrisikoer innenfor 15 av de 19 personvernsklassene definert av Solove [6] og PIA [4] i IdMSet brukt i denne oppgaven

Acknowledgments

This thesis marks the end of a five year study at Gjøvik University College. The work of writing this thesis has spanned over a period of six months, and was finished spring 2012. Many people have been involved and offered both help, motivation and guidance.
I wish to thank my supervisor, Einar Snekkenes, for providing excellent guidance throughout the process of writing this thesis. And also for letting me participate in the PETWEB II-project work.
Thanks to my girlfriend, Ann Kristin Tøfte, for backing me up throughout this process and helping me whenever she could. Ann Kristin has been great at providing motivation and support throughout these five years of studying.
I would also like to thank my opponent and friend, Anders Sand Frogner, for providing comments and useful feedback on my thesis. A thanks also goes out to my other friends at the master information security course in Gjøvik for being sparring partners in discussions and making the time spent writing this thesis a positive experience.
I also wish to thank the members of the PETWEB II-project for allowing me to join the project and providing me with available knowledge and papers. Specifically Lisa Rajbhandari, who provided me with her insight and opinions throughout the process of writing this thesis.
A thanks also goes out to the people who read my thesis and provided me feedback, Ann Kristin Tøfte, Ingvild Bjørklund Wangen, Morten Wangen and Ernst Kristian Henningsen. Your work was very much appreciated, and definetly helped improve my thesis.
A thanks to my family and friends for providing support and motivation throughout these 5 years of studying.
And a thanks to everyone who answered my survey, I hope I did not feed your paranoia too much!
To all those mentioned, and those I forgot to mention, I appreciate all your contributions and this work could not have been conducted without you.

Gaute Bjørklund Wangen, 17th June 2012

Contents

List of Figures

List of Tables

1 Introduction

This chapter contains an introduction to the thesis. It presents the topics covered by the thesis, outlines the problems, and identifies the research questions. The motivations and justifications for conducting the the research are presented. The thesis scope, outline and a summary of contributions is presented at the end of this chapter.

1.1 Topics covered by the thesis

There are three major topics covered in this project; privacy, identity management (IdM) and risk analysis. Privacy is a property which concerns private, often sensitive, information regarding an individual. A person's identity is divided into several partial identities in the sense that a person has different roles in life, such as roles at work, home and leisure. IdM is an administrative area that deals with identifying and managing such identities in a system. Risk analysis is a technique or methodology which is used to assess dangers of events to individuals and/or businesses. Risk analysis is a part of the risk management process. These three topics are used together to solve the main task of this project, which is to discover the risks to privacy posed by the different approaches to identity management. This project intends to discover and investigate these risks through the use of risk management standards combined with different tools for risk identification and analysis.

1.2 Keywords

Risk analysis, Privacy, Identity management (IdM), Identity management systems (IdMS), Privacy Impact Assessment(PIA), Risk IT, Stakeholder analysis, ISO/IEC 27005, MEHARI, Data flow diagram, Threat modeling.

1.3 Problem description

According to Alan Westin [16], privacy can be interpreted as: "... the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".
As our electronic identities expand and increase in complexity, the need for IdM is becoming more apparent. IdMS deals with identifying individuals in a system and controlling access rights

to resources within it. Such systems can i.e. be used as a "Single Sign-On"(SSO), where the system stores information about users to allow them to authenticate only once to access multiple services.
In an information security context the concept of attacker and target is well established, but when privacy is the issue in question, these two concepts may prove too narrow. Personal data has many uses, and the threat to privacy may not always come from what is defined as an attacker. The threat can be someone within the organization lobbying for expanded use of the databases containing personal data, or it can be the IT-department wanting to implement a security measure that unfortunately puts privacy in risk, but increases the security of the organization. This makes the risks posed to privacy in IdM complex and hard to detect. Privacy is also a term that can hold different meaning for people which makes them hard to define. is, i.e. a privacy invasion only related to sensitive personal data or is it something more?
These problems that will be addressed in this thesis using Risk Analysis. The methodologies introduced in this project will be applied as tools to gain a better understanding of risks to privacy, and how to discover these risks.

1.4 Justification, motivation and benefits

The concept of privacy has been recognized since the time of Aristotle, and has been a theme of political debate and philosophical discussions ever since [1]. However, during the last two decades, information technology has rapidly evolved beyond these discussions, and our understanding and protection of privacy is quickly becoming obsolete. Rachels [17] addresses the importance of protecting privacy for individuals in competitive situations, and protecting personal information regarding behavior that would be embarrassing if it becomes publicly known. However, personal data is shared by users every day, and no one knows the ultimate privacy implications of this behavior. To help close this knowledge gap, this thesis addresses methodologies for detecting privacy risks in IdMS.
Identification of risks in IdMS is important to help protect the privacy of individuals, and contribute to the awareness of the user. It is also important to help the vendors of IdMS understand which risks are present in their products. This work can also help developers gain knowledge about the risks associated with IdMS such that they can better protect the privacy of their users.
Detection of privacy risks is a recognized issue within information security, and the "Privacy Impact Assessment" [4] has been around for nearly a decade. This is a standard that has been scoped for detection of privacy issues in information systems, but there exists little research regarding how well this standard perform compared to more established risk analysis standards. There exists many standards and tools for conducting information security risk analysis, most of which are scoped to detect breaches of either confidentiality, integrity and non-repudiation in information systems. These tools have been trialled and tested in their respective areas, but we aim to see how well these established methods work in analyzing risks to privacy.
The work conducted in this thesis can be used as a foundation by other practitioners for choosing a privacy risk analysis approach. It also contributes to the understanding of how IdMS is

vulnerable to privacy violations.

1.5 Research Questions

The identified research questions that are attempted answered in this thesis, are:

1. How does the risk management approaches, "Privacy Impact Assessment(PIA)" and "The Risk IT Framework", compare when it comes to analyzing risks to privacy in a federated identity management system?
2. How can stakeholder analysis be used as a tool to uncover risks to privacy in IdMS?
3. How does the stakeholder approach work to uncover privacy risks in a federated identity management system when compared to a traditional vulnerability identification tool?
4. Within which of the privacy risk classes defined by Solove [6] and PIA [4], can there be detected privacy risks in the federated identity management system using the risk assessment approaches presented in this thesis?

1.6 Scope of the thesis

This thesis uses a federated IdMS as a scenario description, other IdMS approaches are not considered as a part of this project. Figure 1 illustrates the ISO/IEC 27005 Risk management process [7], the scope of this thesis is "Context Establishment" and "Risk Analysis". The other areas of the information security risk management process illustrated in figure 1 will not be addressed. A context establishment is also needed to be able to conduct the risk analysis process. The scenario description in this thesis therefore consist of a context establishment, which holds the necessary information to complete the risk analysis for the two conducted case studies. The risk analysis process will only consider risks that impact privacy. Technical and other system vulnerabilities/weaknesses that have no visible privacy risks are not considered.

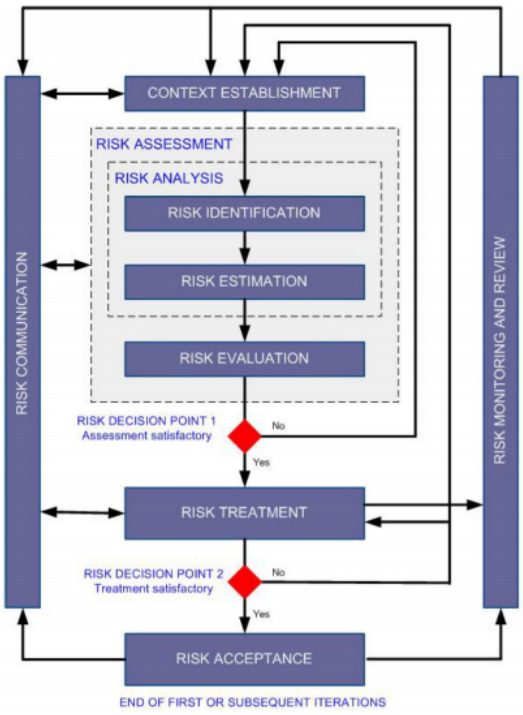


Figure 1: Information Security Risk Management Process. *(Source: ISO/IEC 27005 [7])*

1.7 Thesis outline

This thesis consists of the following chapters:

1. Introduction
2. Related Work: Provides an overview of related work within the research field.
3. Choice of Scientific Method: Consists of the chosen methods for solving the research questions in section 1.5.
4. Context Establishment and Risk Analysis methodologies: Contains a description of methods chosen for context establishment, and a discussion and choice of risk analysis methods for comparison.
5. Privacy Risks for Risk Analysis: Presents the privacy risks that are used in this thesis and impact values of each classification.
6. Stakeholder analysis as privacy threat identification: Presents a methodology for using stakeholder analysis as threat identification.
7. Scenario description: Contains a summary of the scenario description of the IdMS that has

been chosen as case, which is the MinID system by Difi. (The complete description is found in Appendix C.)

8. Case Study 1: A description of conducting risk analysis approach one, Privacy Impact Assessment [4], on the scenario.
9. Case Study 2: A description of conducting risk analysis approach two, The Risk IT Framework [5], on the scenario.
10. Comparison of Results: Contains a comparison of findings using the two different risk analysis approaches.
11. Discussion: Consists of a discussion of results and how these relate to the research questions.
12. Future Work: Describes proposals for future work within the research field.
13. Conclusion: Contains a summary of findings and corresponding conclusions.

This thesis also have 7 appendices:

1. Privacy Impact Assessment Report, produced according to the PIA framework. The PIA report is produced as a standalone document. This report also have appendices produced as a part of the PIA process:
   - Initial Assessment - contains fundamental work for the PIA process and an initial assessment of privacy risks present the IdMS.
   - Project Background Paper - produced according the PIA based on the Initial assessment.
   - PIA Project Plan - The project plan for conducting the PIA.
   - Malicious Stakeholder Actions - Overview of the malicious actions detected as a part of stakeholder analysis in the PIA process.
2. Risk IT report - A simplified Risk IT report, containing risk universe and risk analysis using threat modeling. There is one appendix in this report containing documentation of the threat identification process.
3. Complete Scenario Description - Contains the complete scenario description of MinID, used in both case studies.
4. Stakeholder Analysis - Contains a complete stakeholder analysis of the eight class three stakeholders identified in the MinID system.
5. Questionnaire - Documentation of the survey and results used to determine privacy impacts.
6. Difi Correspondence - Documentation of e-mail correspondence with Difi.
7. Hour list - Documentation of work hours for case study 1 and 2.

1.8 Summary of contributions

In this thesis there was conducted a comparative case study of a federated IdMS using two different risk assessment approaches to analyze risks to privacy. The comparative case study was conducted to determine how well the two risk assessment approaches worked to uncover risks to privacy in IdMS. One risk assessment approach was specifically designed to detect privacy risks (Privacy Impact Assessment), while the other was an established approach to risk assessment (The Risk IT framework). These two approaches to risk assessment are compared using cost-benefit analysis and risk analysis results.
This thesis also contains a presentation of a methodology for using stakeholder analysis to detect privacy risks, and suggests an approach for using stakeholder attributes for likelihood calculations. A comparison of the stakeholder analysis privacy threat identification tool and the more established threat modeling tool, based on the MinID scenario, is also presented.

2 Related Work

In this chapter, the background material and an overview of the research fields related to this project is presented. The purpose of this chapter is to provide the reader with an introduction to the research areas addressed in this thesis. The three main topics of this thesis are (see section 1.1):

- Privacy
- Identity management systems
- Risk management and analysis

To be able to analyze risks to privacy, an understanding of what "privacy" really is, must be established. A problem regarding both privacy and identity is that the terms are not well defined, and different persons may define them in different ways. The meaning of the term privacy is therefore addressed first, and later in an information security context. "Identity" is also a fundamental term of this project. IdM manages the identities of persons, but what is an identity and how can identities in an IdMS constitute risks to invade privacy? To be able to address privacy risks in IdM this thesis outlines what an electronic identity is, and what it contains of. What an IdMS is, and the approaches to IdMS is then addressed. An understanding of IdMS is fundamental in grasping concepts later addressed in the thesis. The different approaches to IdMS are also outlined in this chapter to help the reader understand differences in IdMS and why the IdMS in chapter 7 was chosen.
Related work within the areas of risk management and analysis is addressed in this chapter. Risk analysis is a large part of this thesis, and related work within the fields of risk identification and estimation is therefore visited.

2.1 Privacy and Privacy Risks

The many different aspects related to privacy makes it a wide topic. Privacy can be used in day to day activities, as well as in philosophical, political and legal discussions. It can mean different things to different people, and one of the problems with defining privacy is that different cultures consider the claim to privacy in different ways. What is considered private in Europe, may not be considered private in China or vice verse. To discover the risks to privacy, there must first be established an understanding of what privacy is.

According to Stanford Encyclopedia of Philosophy [1], the distinction between public and private activity was already made in the time of Aristotle. Where private activity was defined as what individuals did in their own home. Public activity was defined as participating in public activities, such as politics. The notion of privacy was already recognized in 2000 B.C., and is still a theme for debate in the present time.
In the book 'Privacy and Freedom' [16], Alan Westin makes one of the better attempts at describing privacy: 'Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.'. This definition of privacy was first published in 1967 and is still valid today.
In Norway there exists laws [18] and regulations [19] that aim to protect the privacy of individuals. The purpose of this law is [18]: "... to protect natural persons from violation of their right to privacy through processing of personal data. This Act shall help to ensure that personal data are processed in accordance with the fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensure that personal data is of adequate quality." This law aims to protect sensitive data from being abused by third parties. The definition of sensitive personal data provided by the Norwegian law is also relevant in the aspect of privacy [18], §2.8: " ... information relating to
a) racial or ethnic origin, or political opinions, philosophical or religious beliefs,
b) the fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act,
c) health,
d) sex life,
e) trade-union membership."
The definitions provided by the Norwegian Government and Alan Westin provides an initial understanding of what the term privacy means in an information security context. Risks to privacy are violations of these rights, where information about the individual is misused in some way.
Understanding risks to privacy is not always a straight forward matter. An understanding of what privacy is has been established, but what risks are there to privacy? And how to recognize them? In his article, "A Taxonomy of Privacy" [6], Daniel J. Solove has created a taxonomy of privacy risks. New technology introduces new privacy risks, and Solove has made an attempt at dissecting and analyzing these risks. He has identified 4 main categories of privacy risks, and within these categories 16 types of privacy risks, illustrated in figure 2. The Privacy Impact Assessment (PIA) Handbook v2.0 [4] also presents definitions of privacy risks in information systems. The definitions provided by PIA overlap with Solove's definitions, but it adds some risks that are not a part of Solove's taxonomy. Both the taxonomy provided by Solove and risks presented by PIA are fundamental in this thesis and is addressed in detail in chapter 5.

One of the main purposes of identity management systems is to store credentials in one place to simplify access to many online services. In his book of pseudo-realism, "Database Nation: The Death of Privacy in the 21st Century" [20], Garfinkel outlines threats to privacy that can occur through the combination of free markets and ubiquitous information technology. Garfinkel points to the dangers of too much surveillance and how this can affect privacy. He points to

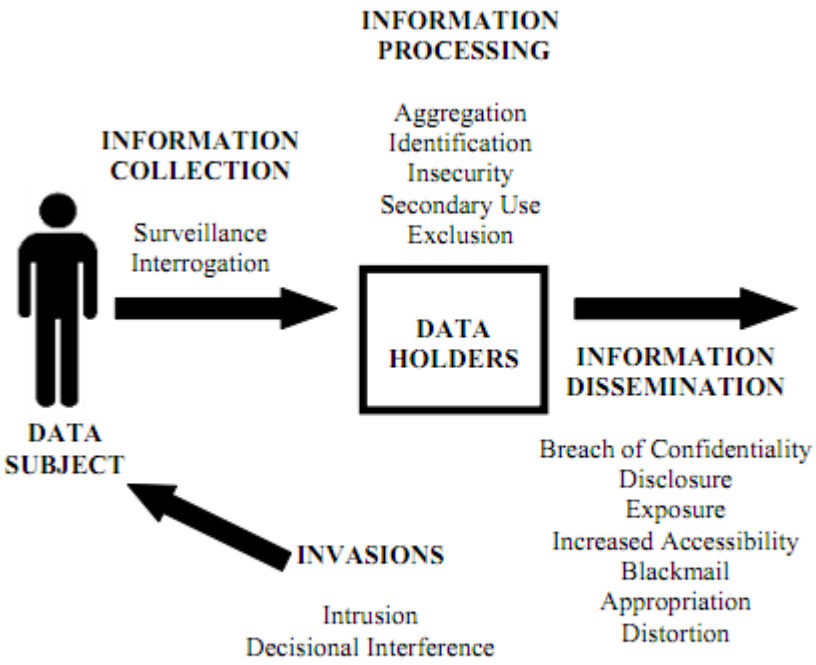


Figure 2: An overview of risks to privacy. *(Source: Solove [6])*

the databases of information now being stored electronically everywhere we go, such as use of credit cards, surveillance cameras, digital medical records and electronically paid toll. All these are making our lives easier in their own way, but they also presents risks to privacy. As Garfinkel points out: "... It's about the woman who's afraid to use the Internet to organize her community against a proposed toxic dump - afraid because the dump's investors are sure to dig through her past if she becomes too much of a nuisance." This example illustrates how easy accessible information can be used against us and pose a threat to our privacy.
In 2011, Paintsil and Fritsch published "A Taxonomy of Privacy and Security Risks Contributing Factors" [21], which is a taxonomy of risk contributing factors for tokens in IdMS. By token they refer to the device that is used to log in to the system, such as a RSA chip or security card. They point to ten risk contributing factors in tokens, and they also present known security and privacy risks in IdMS regarding the use of tokens as guidance for using the taxonomy.
Although the issues of privacy have been recognized for a long time, there is a point in knowing if it is of importance to the common man. In 2007, researchers at the Pennsylvania State University conducted a survey [22] who's purpose was finding out if end users differentiated between computer incidents and threats to privacy. Their hypothesis state that this was the case, and

that the end users often were the weakest link in ensuring security and privacy in computing environments. The conclusion of the study showed: "...that the users are more concerned with security and privacy concerns than they are with other types of computer problems." Which may suggest an increased awareness towards privacy issues, and an indicator that the people are becoming more aware of how helpful technology also may act as intrusive to privacy.

2.2 Identity and Identity Management

Garfinkel [20] points to all the traces of information left behind by users, and how these traces can be tied back to our identity and exploited by third parties. However, storing information at third parties are not always a bad thing. Third parties often store the user information in identity management systems, which is one of the major parts of this project. IdMS are made to make our and the third parties' life easier, one of the main functionalities of an IdMS is to act as a "Single Sign On", where the user authenticates once to access many services. The concept of identity must first be discussed, for within the name of IdM lies a similar problem as with privacy. The word "identity" can mean different things to different people. Identity is a more complex concept than just referring to a person's name. Although a name is one of the things that sets us apart, but that is just a small piece of the picture.

The concept of identity is used to tell people and objects apart, or as a way to define yourself [23]. There are several distinctions that can be made when discussing the concept of identity. Personal identity is one distinction, and is probably what most people would think of when hearing the word 'identity'. But this is not the only way to interpret the term. According to Stanford Encyclopedia of Philosophy [24], there is a distinction between personal, qualitative and numerical identity. Objects can be qualitatively identical when they share a property, but still be very different. The example used in the Stanford Encyclopedia refers to Poodles and Great Danes, they are qualitative identical because they share the property of being dogs. Two poodles will very likely have a greater qualitative identity, but still be different. Numerical identity requires all properties to be equal between two items. For that to happen, both items must be identical in a numerical way (can be expressed in math as 'item a = item b'), and can be counted as one. A more specific approach is needed to apply the concept of identity to computing. The qualitative approach is not adequate in the sense of defining personal identity, it can work in systems such as access control, where access properties are shared by individuals.
Qualitative and numerical are two approaches to understanding identity, but a just as complex issue is defining electronic identities. In the context of identity management the need for a set of properties to define a single object or individual arises. Pfitzmann and Borcea-Pfitzmann [25] have made an attempt at defining identity related to IdM as: "... a set of attribute values related to one and the same data subject." In this context the term 'data subject' is explained as: "... entities being able to interact via communication infrastructures with other entities, i.e. natural and legal persons as well devices used to represent them in interactions. Sometimes, even sets

of persons are called data subject."
An attribute value is explained as a value that can represent its holder in a given setting. The need for these definitions become clear when exploring the subject of electronic identities. As such identities can belong to not just natural persons, but also computers, telephones and other devices. But in the scope of this project, a data subject will refer to natural persons, or groups of persons.
If each valid attribute value connected to the identity is timestamped, then attribute values never change, and further following the reasoning of Pfitzmann and Borcea-Pfitzmann the identity is: "... a set of attribute values valid at a particular time can stay the same or grow, but never shrink." This definition of identity is based on the concept that identities change and grow larger over time. This is an understandable definition, as well as applicable in defining electronic identities.

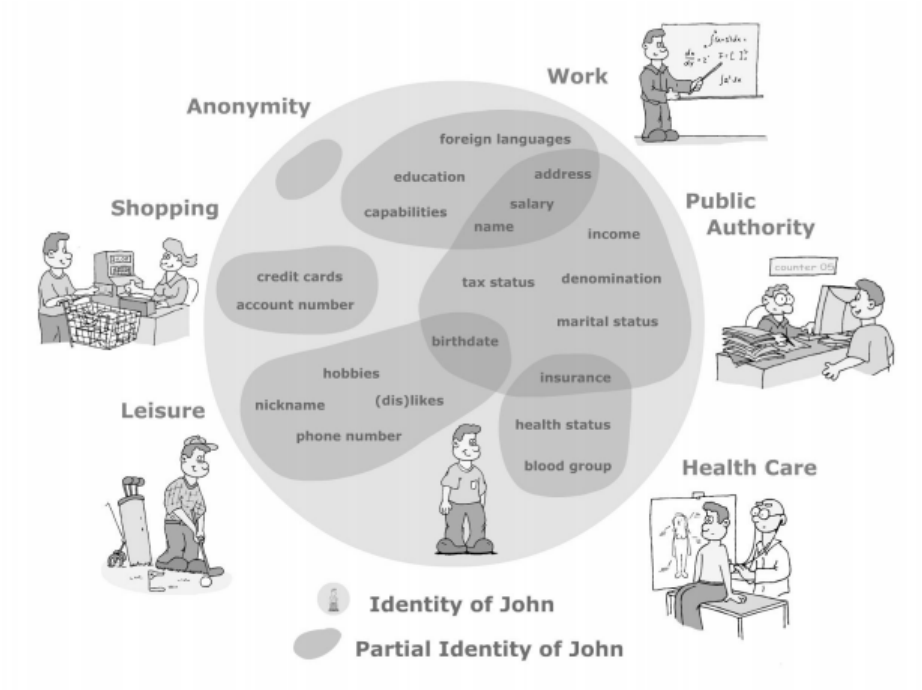


Figure 3: Partial identities of an individual. *(Source:Pfitzmann [8])*

Identity management is an area that deals with identifying individuals in a system. As illustrated in figure 3, a natural person can have several partial identities belonging to his complete identity. According to Pfitzmann and Borcea-Pfitzmann [25], a partial identity is a subset of the identity of an individual. Given that the information about an individual never shrinks, the amount of information gathered about an individual through a whole lifetime will be large. An IdMS is a system that is used to manage all these partial identities as "one identity". The IdMS can according to Pfitzmann be viewed as "... the communication gateway of its user to her/his outside world".
One way of viewing IdMS is as a single sign-on (SSO) approach. According to Pashalidis and

Mitchell [10], the thought behind the SSO is to gather the user's different authentication credentials (partial identities) as one, so that he has to sign in only once to use all of the provided services. The purpose behind this is to increase usability because of the growing amount of network credentials a user has to manage. It is close to impossible to remember every password if the user has a different user name and password at every site. And one of the easiest ways for the user to solve this situation is to apply one common password for every site, which according to Pashlidis and Mitchell, is '... a trade off between security and usability in favor of the latter'.
There are several different developed IdMS solutions available on the market. In their paper, 'Analysis on Identity Management Systems with extended State-of-the-art Id Taxonomy Factors' [9], Srinivasan and Rodrigues outline several of the available approaches to IdMS. The IdMS chosen for the tests, are according to their paper, chosen from the top IdM vendors. The taxonomy of the IdMS is split into two main classifications, 'Features and Capabilities' and 'Strategy and Vision'. Each of the systems are ranked based on their performance in the subcategories within each classification. Of the ranked identity management systems, the ones developed by Oracle and IBM scores best, illustrated in figure 4. This taxonomy is based on the potential of the different systems, and does not consider privacy related issues. The previously discussed paper

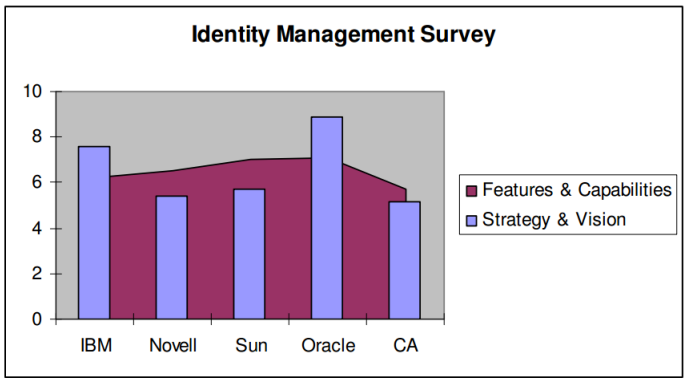


Figure 4: IdM comparison results 2. *(Source: Srinivasan and Rodrigues [9])*

of Pashlidis and Mitchell [10] also addresses the taxonomy of SSO systems. Similar to Srinivasan and Rodrigues's paper, the SSO's are ranked by performance, but the properties and categories used in Pashlidis and Mitchell's paper are very different. The main difference is that Srinivasan and Rodrigues evaluates the performance of developed solutions (i.e. IBM, Oracle), while Pashlidis and Mitchell address the different approaches to IdMS and their performance in different areas.
Pashlidis and Mitchell start off by describing the fundamentals of single sign-on. Using these fundamentals, the properties of each SSO approach is evaluated based on a set of criteria. What is interesting regarding this taxonomy, is that the authors have used privacy and network anonymity as criteria. The authors argue that within the four identified approaches to SSO, only two of them can guarantee privacy. As seen in figure 6, the authors divide the approaches into four different schemes. These schemes are 'Local pseudo-SSO', 'Proxy-based pseudo-SSO', 'Local true SSO' and 'Proxy-based true SSO'. General requirements for being regarded as a SSO in this scheme, is that

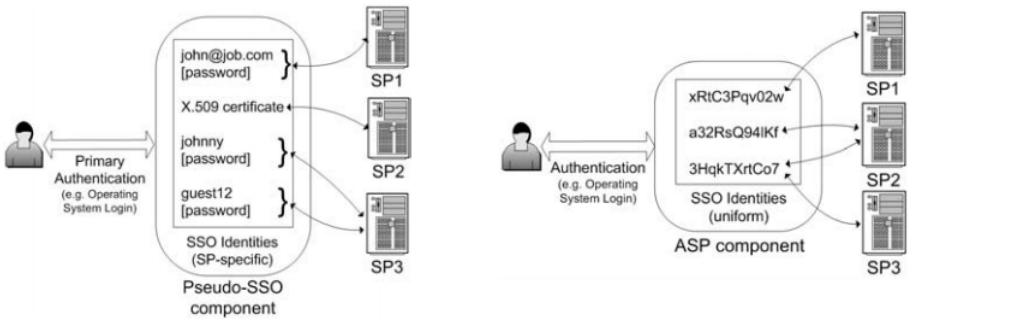


Figure 5: Difference between a Pseudo-SSO and a True SSO(*Source: Pashlidis and Mitchell [10]*)

the user has to authenticate to an ASP (authentication service provider), and the ASP is required to have an established relationship of trust with all service providers if SSO is to be achieved. Supporting infrastructure for secure communication is also needed. What sets these apart is their location and if they are defined as true SSO or pseudo-SSO. The difference between local and proxy-based is that local SSO has a database containing various authentication credentials stored locally, while in the proxy-based SSO, an external server has the role of ASP. The main difference between true SSO and a pseudo-SSO scheme is illustrated in figure 5. In a true SSO a user can potentially choose any identity from his pool of identities (credentials) to use with multiple service providers. While in a pseudo-SSO scheme after the primary authentication of a user, he has to provide separate authentication every time the user is logged into a service provider.
The set of criteria for which each SSO scheme is judged and their associated scores, can be seen in figure 6. The authors conclude that the 'Local true-SSO' and the 'Proxy-based true SSO' schemes are best for providing pseudonymity and unlinkability. While none of the schemes provide anonymous network access, but it can be integrated in the proxy-based solutions.

2.3 Risk Management

Risk can be viewed as the potential for a certain action leading to an undesirable outcome. ISO 31000 [26] defines Risk assessment as "the effect of uncertainty on objectives". The risk management process consists of identification, assessment and prioritizing of risks, which is followed by choosing a strategy and measures for controlling unfortunate events, and maximizing the outcome of opportunities. The risk management process depicted by ISO/IEC 27005 can be seen in its entirety in figure 1.
The scope of this project is risk analysis, which together with risk evaluation, form the process called risk assessment. Risk evaluation consists of evaluating risks according to results from the analysis process, and comparing risk evaluation criteria with risk acceptance criteria. This process should lead to choosing a treatment for each risk. The four risk treatment options described in ISO/IEC 27005 are risk reduction, retention, avoidance and transfer, some form of these options are generally present in all risk management standards. The option chosen in the risk treatment phase should bring the risk down to an acceptable level. The risk analysis process, according to

	Local pseudo-SSO	*Proxy-based pseudo-SSO*	*Local true-SSO*	*Proxy-based true SSO*
Pseudonymity and Unlinkability	cannot be guaranteed	cannot be guaranteed	can be guaranteed	can be guaranteed
Anonymous Network Access	needs additional services	can be integrated	needs additional services	can be integrated
Support for User Mobility	needs additional services	under suitable authentication method	needs additional services	under suitable authentication method
Use in Untrusted Environment	not supported	under suitable authentication method	not supported	under suitable authentication method
Deployment Costs	low	low	high	high
Maintenance Costs	potentially high	potentially high	low	low
Running Costs	low	high	low	high
Trust Relationships	dynamically changing	dynamically changing	concrete and consistent	concrete and consistent

Figure 6: Taxonomy of SSO systems. (*Source: Pashlidis and Mitchell [10]*)

ISO/IEC 27005, is the process of identifying risks and estimating risk. Risk estimates are a result of probability and impact/consequence.

There are many established standards for conducting risk assessment and risk analysis. In the Sandia Report, "A Classification Scheme for Risk Assessment Methods" [11], Philip L. Campbell and Jason E. Stamp make an attempt at classifying these methods. The Sandia classification scheme uses level of detail and type of approach. They use three respective levels, "Expert", "Collaborative" and "Owner", which also reflects the skill level needed to conduct the type of assessment. The "Expert" level assessments need to be conducted by experts within the field, "Collaborative" can be conducted in collaborative between the system owner and a consultant, and the "Owner" class assessments can be conducted by a non-expert. Types of approach presented by Sandia is "Temporal", "Functional" and "Comparative". A "Temporal" assessment simulates and tests key components of attacks to test the system. A "Comparative" assessment presents a risk assessment standard and compares it with the system to this standard to detect flaws or vulnerabilities. The "Functional" approach balances between the "Temporal" and "Comparative" approaches. A "Functional" assessment uses a system-specific understanding of the system, and applies threat models, a list of vulnerabilities, and the likelihood of success of protection mechanisms versus known threats. Figure 7 illustrates the Sandia Report classification scheme, with diverse Risk Assessment approaches categorized in the matrix. As seen in the matrix provided by the Sandia Report, there exists many approaches to risk assessment, and the Sandia matrix only classifies a chosen few of them. A privacy impact assessment [4] is a risk assessment framework developed especially for detecting risks to privacy in information systems. The PIA process can be defined as: "a systematic process for evaluating the potential effects on privacy of a project, initiative, or proposed system or scheme". The PIA is a specifically designed framework for iden-

Level		Approach		
		Temporal	Functional	Comparative
3	Abstract (Expert)	① Engagement Red Team (e.g., IDART™ [22])	④ Sequence AS/NZS 4360 [5] FIPS PUB 191 [14] IAM [21] IEC/ISO TR 13335 [24] Jelen [25] Kaplan & Garrick [27] NIST 800-30 [31] Schneier [37]	⑦ Principles CoCo [10] Freudenburg [16] GAISP [17] GAPP [18] OECD [33]
2	Mid-Level (Collaborative)	② Exercise Force on Force Penetration Testing [15]	⑤ Assistant Manello [29] OCTAVE [2] RAM-W [35] VSAT™ [43]	⑧ Best Practice DOE's 21 Steps [12] e-Commerce [13] ISF [23] ITIL [7] LfLO [28] NIST 800-53 [32] PoLO [34]
1	Concrete (Owner)	③ Compliance Testing security scripts (e.g., SATAN, Nessus) [38] "door rattling"	⑥ Matrix AMSA [4] CRAMM [11] RiskWatch [36] SSAGT [40]	⑨ Audit BS 7799 [6] CobiT® [9] SSAG [39] Trust Services [41]

Figure 7: Sandia Classification Example.*(Source:Sandia Report [11])*

tifying privacy issues in information systems. There exists different approaches PIA. Countries such as Australia, U.K. and Canada, have all developed their own PIA frameworks, based on their own privacy laws and regulations.
In his article, "Should Privacy Impact Assessments Be Mandatory?" [27], David Wright addresses both benefits and disadvantages of the PIA approach to discovering risk to privacy. A PIA can be implemented as a step by step plan (example is provided in the article), and the purpose of this approach is to detect privacy risks and evaluate the seriousness of the risks involved. An ISO standard has also been produced for doing PIA's in financial services, ISO 22307:2008. Wright points to many strengths of the approach, the main points being:

- PIA is good at identifying and managing risks, and can help the company to avoid misjudgment of privacy issues.
- Avoid unnecessary costs and inadequate solutions, PIA helps to prevent unnecessary costs related to privacy regarding inadequate solutions and implementations.
- General security improvements regarding personal data handling.

While the main drawbacks Wright mentions for these methods are; adding the bureaucracy of decision making, delays in implementation of projects and add additional costs as the main arguments against PIA.
Since this is an approach that has been specially developed to find risks to privacy, it will be the

main approach to risk analysis in IdMS. The PIA framework chosen for this thesis, is the PIA that has been published geographically closest to Norway, which is the UK version. This framework is also still "new" since it was published in 2009.

2.4 Risk Analysis

According to ISO/IEC 27005 [7] the risk analysis process consists of risk identification and estimation (see figure 1), which is also the definitions used in this project. Privacy threat identification is one of the larger parts of this project, and is therefore addressed in this section. Syalim et.al. [28] provides a comparison of four established risk analysis methods, which together with the overview of risk assessment methods published by ENISA [13], provides basis for choice of risk estimation. The ENISA guide is more extensive than Syalim et.al., and also rates the different approaches according to their quality in threat identification, threat characterisation, exposure assessment and risk characterisation. ENISA also addresses the skills needed for conducting each method.

2.4.1 Threat Identification - Stakeholder Analysis

The concept of stakeholder theory has been around since Freeman published his book, "Strategic Management: A stakeholder Approach" [29], and is "the Principle of Who or What Really Counts" in an organization. The plan of this thesis is to use stakeholder analysis as a means to identify threats to privacy.
Before going into stakeholder analysis, a definition of the word "stakeholder" is needed. There exists many different definitions of a stakeholder, most of which centers around who or what really counts in a project. Mitchell et.al. provides several definitions of what a stakeholder can be, i.e.: "... a person, group, neighborhoods, organizations, institutions, societies and even the natural environment are generally thought to qualify as actual or potential stakeholders." This provides an insight to what kind of entities stakeholders can be, but it does not define the term properly. R. Edward Freeman's [29] defined the term stakeholder as: "A stakeholder in an organization is (by definition) any group or individual who can affect or is affected by the achievement of the organization's objectives". This is a wide definition, and one might argue that this includes too many entities as possible stakeholders, but it provides the reader with an understanding of what a stakeholder is.
The process of identifying stakeholders have later been named stakeholder analysis. This concept was elaborated by Mitchell et.al. [12] in 1997, which proposed to classify stakeholders with the attributes "power" ,"legitimacy" and "urgency". This three categories define "the degree to which managers give priority to competing stakeholder claims" [12]. Power in this sense is defined as the stakeholders ability to force his will upon another stakeholder, and make the other stakeholder do something he would otherwise not have done. Legitimacy is based on the stakeholder's relationships with other stakeholders within the organization and the organization itself. Ur-

gency is based on the urgency of the stakeholder's claim in and for the organization. These three attributes are used to classify the stakeholders according to figure 8. In 2004, J. McManus pub-

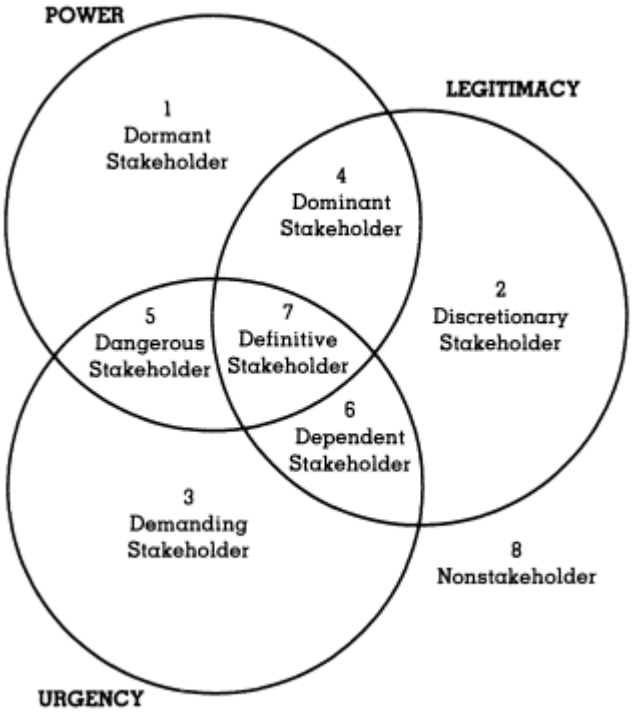


Figure 8: Stakeholder classification. *(Source: Mitchell et.al [12])*

lished his article "A Stakeholder Perspective within Software Engineering Projects" [30], which takes the stakeholder analysis process one step further, and scopes it for software engineering. McManus argues for the importance of stakeholders in software engineering projects, and that successful software engineering projects rely on stakeholders caring for the project. McManus proposes a method for stakeholder identification based on an article published by the The World Bank [31].

Pacheco and Garcia [32] published an article in 2009 that compares methods for stakeholder identification. The previously mentioned article by Mitchell et.alMitchell:1. is among the methods that are compared in the article. Pacheco and Garcia compares the stakeholder identification methods through methodical reviews of available literature. The criteria used in the comparison are "Role Establishment", "Stakeholder Skills Analysis", and "Allocation of Requirements Priorities". Role establishment refers to establishing the role of the stakeholder within the project. Stakeholder skills analysis is important in order to determine abilities, skills, knowledge and experience of the stakeholders. And Allocation of Requirements Priorities is the process of prioritizing requirements from the stakeholders. One of the strongest methods from the comparison in the Pacheco and Garcia paper, was the one proposed by McManus [30] One thing to mention about the methods suggested by Pacheco and Garcia [32], is that the methods are not always

"methods" for doing a stakeholder analysis. What is meant by this is that there is discussion regarding stakeholders in the documents, but few concrete "step by step" plans for identifying stakeholders which are easy to follow. McManus states that one of the reasons for this might be: "What practitioners do know is that stakeholder involvement is generally context-specific; what works in one situation may not be appropriate in another."

2.4.2 Threat Identification - Threat Modeling

A more established approach to threat identification, is the data flow diagrams, explained in the paper "The Semantics of Data Flow Diagrams" [33]. DFD is commonly used in designing information systems, and modeling the process aspects of the information system. DFD is used to illustrate flows of data between processes, data sources and external agents. Using the DFD approach as a means of threat identification is called "threat modeling". Steven F. Burns from the SANS Institute has published an article that offers guidance in the field of threat modeling using DFD called "Threat Modeling: A Process To Ensure Application Security" [34]. The Burns paper outlines how to model the system for information security, and how to identify threats using threat modeling. Within the same topic, Swiderski and Snyder published the book "Threat Modeling" in 2004 [35], which offers a structured approach for identifying, evaluating, and mitigating risks to system security. Both the approaches urges the practitioner to assume the role as the attacker, and try to imagine what can go wrong when analyzing the system. The concept of threat modeling and identification, is explained in further detail in chapter 4.

2.4.3 Risk Estimation

The risk estimation process generally consists of a calculation of probability (likelihood), together with a determination of impact to the organization. Some of the risk assessment frameworks come with their own tools for calculating probability(i.e. MEHARI [14]. But in frameworks such as Risk IT [5], it is recommended that the probability calculation of an event occurring is based on historical numbers. If no such data is available, there exists other approaches to determining probability, such as Interval Analysis [36] and Bayesian probability [37]. MEHARI [14] suggests determining intrinsic likelihood and subtracting estimated efficiency of controls to determine residual likelihood.
Impact of a risk is generally measured in damage to the organization or loss of assets. Risk evaluation, or seriousness, is generally computed using likelihood and impact to the organization. Frameworks such as ISO27005 [7] and Risk IT [5,15] recommends displaying the risk evaluation in a matrix for illustrative purposes.

3 Choice of Scientific Method

The methodology for solving each research question from section 1.5 is addressed in this chapter. The possible methods for solving each research question is discussed, and the chapter is ended with a conclusion of chosen approaches. The different scientific methods that are considered for solving the research questions, are briefly discussed before addressing each research question.

The two main approaches to research is called "Quantitative" and "Qualitative". The **Quantitative research** approach is to base the conclusions on amounts, or quantities, of data [38]. This is the conventional way to approach research. The **Qualitative research** approach is used for looking at characteristics, or qualities [38]. The qualitative approach is generally used for social sciences, with the aim of understanding phenomenons such as human behavior and the underlying reasons.
Scientific **interviews** is a qualitative approach to solving a problem [38]. It should be performed as a face to face interview, with some questions outlined in advance.
Surveys is a quantitative approach [38] for gathering data can easily be used for statistics. Online surveys allows for easy access to the survey itself, this approach can yield big quantities of relevant data.
Scientific **Modelling** is the process of generating a model to help solve a problem. The models are mainly used to model either phenomena, data og theory [39]. As this method investigates a particular phenomenon, it is mostly a qualitative approach.
A **Case study** is according to Flyvbjerg [40]: '...an intensive analysis of an individual unit (e.g., a person, group, or event) stressing developmental factors in relation to context.' The strengths of case studies is that they can explore a concept in depth and it has a high conceptual validity.

3.1 Research question 1

Research question 1 states "How does the risk management approaches, "Privacy Impact Assessment(PIA)" and "The Risk IT Framework", compare when it comes to analyzing risks to privacy in a federated identity management system?". The purpose of this question is to compare a specialized method for privacy analysis to an established method for risk analysis. The purpose of this is to see how well the two approaches work to detect privacy risks in identity management systems.
One possible approach to solving this question is to perform scientific interviews. What makes this approach difficult is the lack of knowledgeable persons. There probably exist people who has knowledge within the different fields, such as uncovering privacy risks using one of the men-

tioned approaches. It is a long shot to hope finding people who are knowledgeable within both standards, privacy risk, and has used them in coherence with identity management systems. This makes interviews an unrealistic approach. Surveys are also unrealistic as there is not many people who possess the described expertise. The results from such a survey would probably consist of different subjective estimates, and would not be useful.
Modeling the identity management is a feasible approach. Modeling a federated IdMS is possible, but it is not certain that the model will contain the information necessary to conduct both risk assessments. Another possible approach is the comparative case study, where the two risk assessments are performed on the same scenario description. Doing this will yield comparable results since they are performed on an identical scenario. Modeling can also be used as a tool in the scenario to portray the system. Creating a scenario description of an IdMS, and performing a comparative case study, seems like the most feasible approach.
To create a scenario description of an IdMS, documentation about the system is needed. The alternatives is either to construct an entirely fictional scenario based on one of the approaches presented in section 2.2, or to base the scenario on an existing approach. The prerequisite for doing the latter is that there exists a possibility of obtaining documentation about a system. Basing the scenario description is the preferred approach, as this is likely to result in less guesswork together with this approach being less dependent on the skills of the authors.

Conducting depth interviews with experts to map risks to privacy in information systems is a viable approach, but conducting interviews is a time consuming progress. Developing depth interviews, finding experts and making appointments might prove to be too much work for the time available to conduct this project. There exists a body of literature on the subject of privacy risks, and it is a better option to use this as foundation for privacy risks. The time usage and results from a depth interview is not likely to justify the results, when compared to studying related work.
Since the research question state risk analysis, impact to privacy must also be addressed. The approach decided upon is to use privacy risks found in related literature. The question still remaining is how to determine impacts to privacy from the different risks? To be able to determine anything about impact of privacy risks on a natural person, there is a need for an objective source of information. Although it is possible to model how a threat can impact privacy, applying a measurable scale of "how much it hurts" based on the model would probably not yield accurate results. The same goes for case studies, it is possible to conduct a case study for each identified risk, but this would give a large amount of case studies, and be unrealistic for this thesis.
Conducting scientific interviews would help determine the severity of each risk, but this issue is just as much about quantity of answers. This is because privacy risks concerns all of us, and there is a limit to how many scientific interviews that can be conducted. A more quantitative and less time consuming approach to determining privacy risks is the survey. The survey can be used to address each privacy risk. Such a survey can also be used for both case studies, although the risks will not be specific for each threat scenario, it can constitute a "worst case" impact when categorizing the privacy risks.

3.2 Research question 2

The second research question state "How can stakeholder analysis be used as a tool to uncover risks to privacy in IdMS?". The thought behind this research question is to develop an approach where stakeholder analysis can be used to detect privacy risks in IdMS. PIA emphasizes doing stakeholder analysis and conducting interviews with the stakeholders. However, the literature regarding stakeholder analysis as a privacy risk identification tool is very limited, as well as the practitioners opportunity for stakeholder consultation. The developing of a stakeholder analysis method is the approach chosen as a foundation for solving research question 3 and 4.
Doing surveys is not a feasible approach since this research question relies on the development of an approach. Attempting to solve this problem with interviews will have the same problems regarded to knowledge as described in method for research question 1, section 3.1.
Using related theoretical work is a possible approach, as there exists closely related work within the area ([30, 31, 41] and others). None of which are scoped specific for the purpose of this research question, but they provide a foundation for solving this question. The stakeholders can be identified using the scenario description developed as a part of research question.

3.3 Research question 3

The third research question is formulated as "How does the stakeholder approach work to uncover privacy risks in a federated identity management system when compared to a traditional vulnerability identification tool?". The thought behind this is to experiment with the two chosen approaches for privacy risk identification on the scenario description developed as a part of the previous research question. The desired result is to define a context for which these methods can be applied, such that others with similar cases/scenarios might use this method to obtain valid results. The validity of the approach developed as a part of the previous research question 2 is also to be tested.
Interviews could be conducted to obtain an initial understanding of privacy risks in IdMS, but surveys and interviews are very time consuming to perform, and there is a time constraint on this project. Which, combined with the workload presented in the other research questions, leaves these options as less applicable for solving a part of this question.
Since this question relies on the previous work of this project and further experimenting on the case, a valid approach that can be integrated with the rest of the thesis is to conduct two case studies based on the scenario description, where the two tools for detecting privacy risks can be integrated in the risk assessment standards.

3.4 Research question 4

The fourth research question is formulated as "Within which of the privacy risk classes defined by Solove [6] and PIA [4], can there be detected privacy risks in the federated identity management system using the risk assessment approaches presented in this thesis?". The purpose of this question is to analyze the privacy risks found in the scenario description, using the risk identification tools and the privacy risks in information systems developed as a part of solving research question 1.

3.5 Metrics for comparison of Risk assessment approaches

Determining metrics for comparison of two different approaches to risk assessment is not obvious. Comparing the frameworks on quality of the risk analysis results is not feasible, as this will depend entirely on the subjective opinions of the practitioners.
Another qualitative approach is to evaluated each approach. The frameworks can be evaluated on layout, usability, methodology and findings. Which is a feasible approach for this thesis.
A quantitative approach for comparing the frameworks and methods, is the cost-benefit analysis. This approach can be used to compare quantifiable data from both approaches, and is the chosen approach for comparing findings from the case studies. The following metrics were used for comparison:

- Time use: How much time was spent conducting each approach.
- Privacy risk scenarios: The amount of privacy risk scenarios detected using each threat identification approach.
- Privacy risks: The amount of privacy risks detected for each method. (Limited to two privacy risks per scenario)
- Privacy risk distribution: How the detected privacy risks were distributed, using the presented "Privacy Risks for Risk Analysis" found in chapter 5.

Example of what the cost benefit analysis looks like is seen in figure 9. Results from the risk analysis process will also be compared, and an example of this approach can be seen in 10.

Method	Time Use	Privacy Risk Scenarios Detected	Privacy Risks Detected	Additional gains
Method 1	*X hours*	*X amount of scenarios*	*X amount of risks*	*Other benefits...*
Method 2	..	...	...	...
...	...	...	...	...

Figure 9: Example of cost benefit analysis table.

Some weaknesses are present when conducting the comparison using these metrics. Such as the

Privacy Risk Class	Method 1 Detected Amount	Method 2 Detected Amount	Risk Severity
Privacy risk 1	*5*	*7*	*8*
Privacy risk 2	*4*	*2*	*5*
...	...	...	...
Total amount	*xx*	*xx*	-

Figure 10: Example of comprison table for Risk Analysis results.

time difference between the comparisons of two approaches having a time difference, because of the familiarity of the system when conducting the second analysis. Meaning that case study 2 will be conducted using less time. This issue is discussed together with the comparison.

In addition to these metrics, the PIA provides its own "metrics" for measuring performance. These ideal results will also be discussed, to see if PIA delivered in our case study (this discussion will be exclusive for PIA). As a result of a properly conducted Privacy Impact Assessment the ideal results, according to the Handbook, can be [4]:

1. "the identification of the project's privacy impacts;
2. appreciation of those impacts from the perspectives of all stakeholders;
3. an understanding of the acceptability of the project and its features by the organizations and people that will be affected by it;
4. identification and assessment of less privacy-invasive alternatives;
5. identification of ways in which negative impacts on privacy can be avoided
6. identification of ways to lessen negative impacts on privacy;
7. where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them;
8. documentation and publication of the outcomes."

3.6 Conclusion

The determined approaches used to solve the research questions in this thesis are:

- Research question 1 - Comparative case study conducting the two risk assessment approaches on the same scenario description. The scenario description is to be based on an existing IdMS. Privacy risks are addressed using related work. The comparison of the two risk assessment approaches will be conducted using one qualitative approach, where the standards are compared and evaluated on layout, usability, methodology and findings. And one quatitative approach based on cost-benefit analysis.

- Research question 2 - Development of the stakeholder analysis tool will be founded on related theoretical work.
- Research question 3 - The two tools for privacy threat identification is to be integrated in the comparative case study, one tool in each of the risk assessments.
- Research question 4 - Will be solved using results obtained from work conducted in this thesis.

4 Context Establishment and Risk Analysis Methodologies

This chapter consists of the chosen approaches for context establishment and risk analysis, together with the metrics and arguments for choosing. "Context establishment" is the term used by ISO/IEC 27005 [7] (see figure 1, and describes the boundaries for which the risk assessment process is to take place.
The main choices of this chapter were "MinID" [2] by the Norwegian Agency for Public Management and eGovernment [3] as scenario for both the assessments. The Privacy Impact Assessment [4]does not specify approaches to stakeholder or risk analysis. And the ISO27005 compliant risk analysis tool MEHARI [14] was chosen for PIA, while the tools found for conducting stakeholder analysis were not found adequate for privacy threat identification purposes.

4.1 Choice of IdMS for Comparative Case Study

There exists many approaches to IdMS (see section 2.2). As this the main theme in this thesis is privacy, it was important that the IdMS handle personal data. And that the system was of Norwegian origin, or more importantly, in use in Norway. The system should also be a federated system.
For relevance to future risk assessments of IdMS, the chosen system should be based on an approach that is likely to be used in the future. The IdMS should therefore be based on one of the systems presented in the taxonomy of IdMS provided by Srinivasan and Rodrigues [9] (see figure 4), as these are "state of the art"-approaches to IdMS. And the IdMS chosen should also qualify as a "True-SSO" according to the taxonomy of SSO systems by Pashalidis and Mitchell [10] (see figure 6).
Three suitable candidates were found, all members of the Norwegian "ID-portal" federation, which provides access to several public services. Two of the three IdMS are privately owned, and do not have openly available documentation for their solutions. Trying to acquire documentation on privately owned IdMS solutions may prove difficult as they will be interested in protecting their design secrets. The government owned solution was therefore the most interesting candidate for the scenario. This solution is called MinID [42] and is designed and operated by the Agency for Public Management and eGovernment (Difi) [3]. Difi is bound by the law of transparency [43] (Offentleglova), which says that every Norwegian citizen has right of access to documents, journals and the likes in public administration, and the purpose of this law is to make public organs as transparent as possible. In practice, this means that documentation about the system should be available in the public domain, as Difi is bound by law to provide it. This opened the possibility of founding the scenario description on open sources. Since the time limit

of this project is 6 months, using open sources relieves the authors of external dependencies. There are some drawbacks of using open sources, such as obtaining information about i.e. the security measures and content of databases may prove to be difficult, as Difi is not likely to openly share documentation regarding their intrusion detection system or firewall settings.
MinID uses OpenSSO from Oracle as identity federation platform [44]. The solution from Oracle is a part of the state of the art taxonomy by Srinivasan and Rodrigues [9], and is one of the best choices for IdMS platform according to the taxonomy. MinID is, according to our understanding, classified as a "Proxy-based true SSO system", and is also within the taxonomy provided by Pashalidis and Mitchell [10].
To add to the relevance of choosing MinID as IdMS as scenario, it was at the time of this thesis the biggest IdMS in Norway, used by over 2 million Norwegians [45] (from a total population of about 5 millions). MinID qualifies within all criteria for choosing IdMS and is chosen for the scenario description.

4.2 Case study 1 - Privacy Impact Assessment

The Privacy Impact Assessment is a standard used to detect risks to privacy in systems or projects that handle privacy related information. This document uses the Privacy Impact Assessment Handbook Version 2.0, published by ICO. According to Abu-Nimeh and Mea [46], PIA is, within the Sandia risk classification scheme, regarded as an "Assistant" method. From the Sandia Report [11]:
"An Assistant method type keeps track of things, of details, the way a good human assistant does. In this case the assistant keeps track of combinations of lists such as threats, vulnerabilities, and assets. The best instances of this type "walks" the user through the process, prompting for the input needed to populate and rank each list. The lists are combined and ordered mathematically, or at least in some explicit way, usually defined by the user. The ordered lists, which include primarily a list of vulnerabilities and, hopefully, a list of remedial actions, are the result of using the type."
The PIA framework is specially designed to detect risks to privacy in systems that handle personal data. It is recommended by the framework to conduct the PIA in the starting phase of the project, before the project is implemented, where the PIA can make a real impact on the project. This did not concern this thesis, as the goal of this project was to check how the PIA actually detects privacy risks when compared to another more established risk assessment standard. This project does not aim to force any changes in the case study, it is only used for testing the framework and comparing the results to another framework, to see if the specialized framework for detecting privacy risks performs better.

The Handbook describes the PIA process divided as into five major steps (illustrated as a process in figure 12. These five steps are described below. What the handbook does not mention in this step-by-step plan, is the initial assessment that should be conducted before performing the preliminary phase.

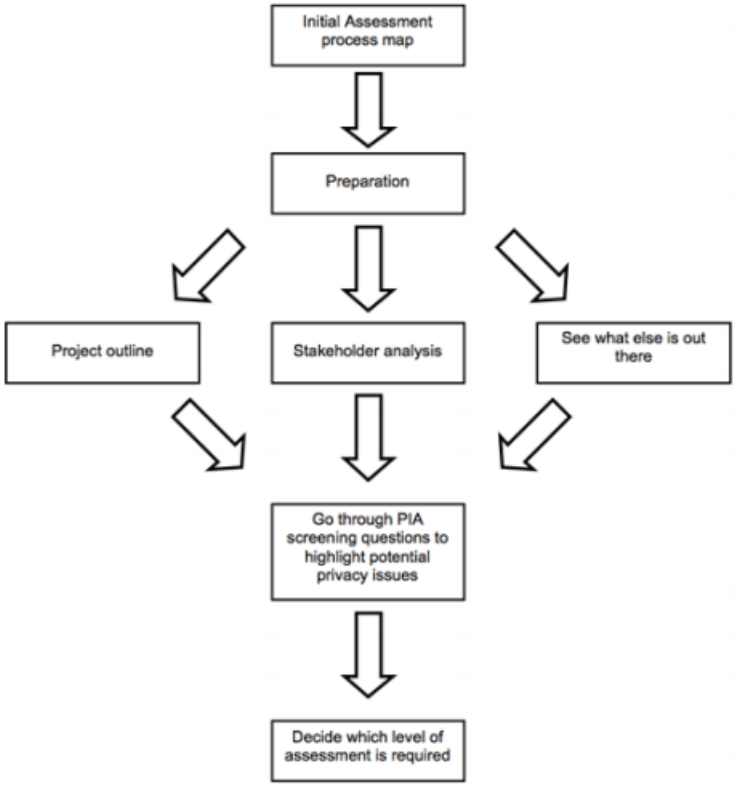


Figure 11: The Initial assessment process map. *(Source: PIA [4])*

There are three pieces of information needed for the initial assessment; a project outline, a stakeholder analysis and environmental scan. This information is used to answer the screening questions found in Appendix 1 of the PIA framework. These are superficial questions regarding the system and how it handles privacy related information. The conclusion from this process will determine what type of PIA is to be conducted. Possible types are full scale, small scale, privacy law compliance check and Data Protection act compliance check. What separates the full scale and small scale assessments is that the small scale PIA is less formalized and involves less investments. Both the PIA processes consists of the same five steps, but the small scale are less extensive. The privacy law compliance check is the process of checking that the project, the personal data it handles and the business processes it uses are compliant with all relevant laws, such as governance laws [47], laws of electronic communications [48] and The Human Rights Act [49]. A data protection act compliance check is conducted in order to ensure that the project is compliant with the Data Protection Act (called "The Personal Data Act" in Norway [18]).
The initial assessment process is important because the rest of the work conducted in the assessment is founded on the initial assessment together with the project background paper from the preliminary phase. The five major steps of PIA are [4]:

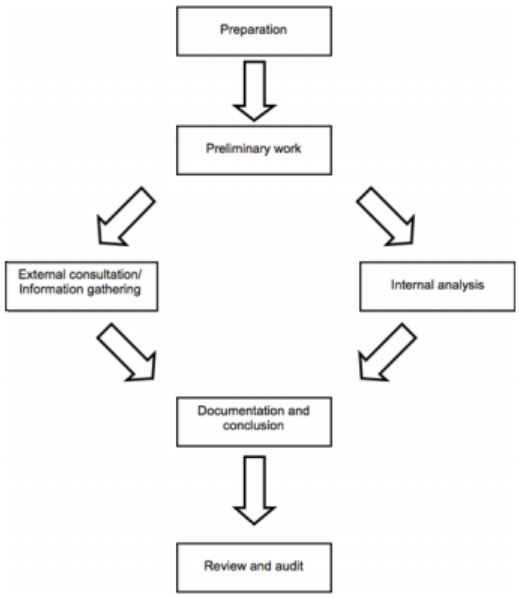


Figure 12: Full scale and small scale PIA process map.*(Source: PIA [4])*

1. Preliminary Phase: The purpose of this phase is to establish a basis for the PIA to be conducted efficiently and effectively. It consists of:
   - information gathering, i.e. acquiring system documentation, project initiation documents, project plans...
   - develop project outline (for conducting PIA.)
   - Scoping and delegating resources for conducting the PIA
   - Preparation of the project background paper (used to establish a basis for discussion with stakeholders and an initial assessment of potential privacy risks present in the system).
2. Preparation Phase: This phase is used to make the arrangements needed to enable the critical phase three to run smoothly. Consists of:
   - developing a consultation plan to ensure that discussions with stakeholders are effective.
   - Form a PIA consultation group (PCG). This comprises representatives of stakeholder groups.
   - Distribute the project background paper to the PCG. This ensures that the PCG members can understand the nature of the proposal.
3. Consultation and analysis phase: The purpose of this phase is to ensure that problems are identified early, and that effective solutions are found. Consists of:
   - consulting with stakeholders.
   - conducting risk analysis.
   - identifying privacy related problems.
   - search for solutions.
4. Documentation Phase: Purpose is to show that the PIA process was performed appropriately, provide basis for reviews and audits, and documentation in general. Consists of:

- documenting all prior activity
- Producing a PIA report
- reviewing and publishing the PIA report

5. Review and Audit Phase: The purpose of this phase is to ensure that the undertakings arising from the consultation and analysis phase are carried through into the running system. Consists of:
   - Implementing mitigation measures identified as part of the PIA process
   - Reviewing systems and documenting
   - Create privacy review report and publishing

4.2.1 Justification for using PIA on MinID

The framework recommends that the PIA should be conducted at an early stage in the project life cycle, ideally before the system is implemented. But the framework also states [4]: "If the project is underway, start today, so that any major issues are identified with the minimum possible delay." This is interpreted as that the PIA can be conducted at a later stage in the project life cycle. The Handbook also states that the PIA can be conducted by an external consultant, which is the role the practitioners in this thesis has assumed. The framework states that a PIA is recommended for assessing common functions in government, and it states that PIAs are well suited for assessing areas such as identity authentication and identity management.

4.2.2 Stakeholder Analysis in PIA

To perform a stakeholder analysis, the important stakeholders for the project needs to be identified. To choose methodology for stakeholder identification for PIA, the McManus [30] approach was chosen. This method is easy to follow and outlines a step by step approach for stakeholder identification. It is also one of the strongest approaches to stakeholder identification according to Pacheco and Garcia [32].
The stakeholder identification process described by McManus [30] is adapted from The World Bank [31], and is as follows (described as steps):

1. Who might be affected (positively of negatively) by the development concern to be addressed?
2. Who are the "voiceless" for whom special efforts may have to be made?
3. Who are the representatives of those likely to be affected?
4. Who is responsible for what is intended?
5. Who is likely to mobilize for or against what is intended?
6. Who can make what is intended more effective through their participation or less effective

by their non-participation or outright opposition?

7. Who can contribute financial and technical resources?
8. Whose behavior has to change for the effort to succeed?

The guidance provided by McManus was also used when the stakeholders were categorized. Given the number of stakeholders that could be detected, a methodology for visual representation of the stakeholders were needed. Representing the stakeholders as a tree structure is a comprehensive way of visualizing the stakeholders, a tree structure of three levels should be sufficient for the stakeholder analysis.

For analysis of each stakeholder, a more extensive tool than the McManus method was needed. The McManus method only described what is supposed to be found, but not so much how to find it. It also lacks a formal way of representing the stakeholders and their properties. This was also a consistent problem with the methods that was looked through of the suggested methods from Pacheco and Garcia [32]. Literature for performing the stakeholder analysis was found, but much of it suffered from being too general (i.e. McManus [30]) or too wide-ranging (Mitchell et.al. [12]), and none of them were scoped for identity management systems or to detect privacy risks. The tools that were found differed both in quality and complexity, the tool that was chosen for adaptation was Kammi Schmeer's "Stakeholder Analysis Guidelines" [41]. This tool was scoped for its' respective area (health policies), but Schmeer has a step-by-step approach which is easy to follow and adaptable for this case.
The purpose of this stakeholder analysis was to determine the following attributes of each stakeholder:

- what positions each stakeholder have
- their importance for the project
- capabilities
- incentives
- their assets
- their knowledge
- relationship with other stakeholders
- consequences regarding assets if the stakeholders choose to act on their capabilities
- conflicting interest regarding personal data, threatening privacy and creating a risk

To reduce complexity of the stakeholder analysis, stakeholders with equal or similar capabilities and assets should be grouped together. The time frame for the project put limitations on both the complexity and scope of the stakeholder analysis. Schmeer [41] also comments on the impor-

tance of setting a limit of stakeholders. If the amount of potential stakeholders is too large, they need to be prioritized. The stakeholders can be ranked by their importance and influence in the project, the ones defined as trivial or unimportant for the project, can be left out of the analysis.

The methods that were found for conducting stakeholder analysis were not specifically designed for IdMS and privacy risks. Another problem with the discovered tools and methods was that they were vague and hard to follow. The existing tools and methods were not found sufficient for our purpose of using stakeholder analysis as a tool for privacy threat identification. These are the reasons for not using an established method for stakeholder analysis, and instead creating a new method based on previous work by others.

4.2.3 Choice of Risk Analysis tool for PIA

PIA is a framework for the risk assessment process, and it does not specify tools for the risk analysis. Choosing risk analysis tool is therefore left to the practitioner to decide. In choosing a tool for risk analysis, the main criteria was that the tool should be ISO/IEC 27005 compliant and open source. Syalim et.al [28] has published a comparison of risk analysis methods, which compares four methods for risk analysis based on the four basic steps of the risk analysis process (see section 2.4). The four methods compared are MEHARI, Magerit, NIST SP800-30 and Microsoft's Security Management Guide. None of the methods compared in the paper stood out as superior to other method, but the impression was that all of the tools were of high quality. The next step in choosing a method was to check the four methods in the ENISA [13] framework, where MEHARI, Marion and NIST SP800-30 are assessed (see figure 13). Marion has, according to ENISA, been replaced by MEHARI, which leaves SP800-30 and MEHARI. Both these methods score similarly, but SP800-30 is also a tool for risk management, while MEHARI is a specialized risk analysis tool. MEHARI (MEthod for Harmonized Analysis of RIsk) by CLUSIF [14] was chosen as the risk analysis tool to be adapted to case study 1. It is an open source tool (there is a mistake in the ENISA report [13], figure 13, where it says that MEHARI costs money), and according to Syalim et.al [28], the tool has no shortages when compared to the other risk analysis methods in the paper. The MEHARI risk analysis was originally designed to assist Chief Information Security Officers in their information security tasks [14]. Figure 14 shows the process of determining risk seriousness using the MEHARI tool. The goal of the MEHARI risk analysis is to determine risk seriousness. This is illustrated in a matrix using residual likelihood and impact. Residual likelihood is a result of the intrinsic likelihood (which is the total likelihood of an event occurring without any preventive measures), and the effect of existing risk reduction measures. Residual likelihood is calculated the same way, using intrinsic impact and efficiency of existing security measures.

Attributes / Products	Threat identification	Threat characterisation	Exposure assessment	Risk characterisation	Risk assessment	Risk treatment	Risk acceptance	Risk communication	Languages	Price (method only)	Size of organisation	Skills needed[6]	Licensing	Certification	Dedicated support tools
Austrian IT Security Handbook	••	•	•	••	•••	•••	•••	•••	GE	Free	All	**	N	N	Prototype (free of charge)
Cramm	•••	•••	•••	•••					EN, NL, CZ	Not free	Gov, Large	***	N	N	CRAMM expert, CRAMM express
Dutch A&K analysis	•••	•••	•••	•••					NL	Free	All	*	N	N	
Ebios	•••	•••	•••	•••	•••	•••	•••	•••	EN, FR, GE, ES	Free	All	**	Y	N	EBIOS version 2 (open source)
ISF methods	•••	•••	•••	•••	•••	•••	•••	•••	EN	For ISF members	All except SME	* to ***	N	N	Various ISF tools (for members)
ISO/IEC IS 13335-2 (ISO/IEC IS 27005)	••	••	••	••	••	•••	•••	•••	EN	Ca. €100	All	**	N	N	
ISO/IEC IS 17799	•					•			EN	Ca. €130	All	**	N	Y	Many
ISO/IEC IS 27001						•	•		EN, FR	Ca. €80	Gov, Large	**	Y	Y	Many
IT-Grundschutz	•••	•••	•••	•••	•••	•••	•••	•••	EN, GE	Free	All	**	Y	Y	Many
Marion (replaced by Mehari)	•••	•••	•••	•••					EN, FR	Not free	Large	*	N	N	
Mehari	•••	•••	•••	•••					EN, FR	€100-500	All	**	N	N	RISICARE (ca. € 10.000)
Octave	••	••	••	••	••	••	••	••	EN	Free	SME	**	N	N	
SP800-30 (NIST)	•••	•••		•••	•••	•••	•••		EN	Free	All	**	N	N	

Figure 13: Summary of Risk Analysis Comparison. *(Source: ENISA [13])*

4.3 Case Study 2 - Risk IT

The Risk IT Framework [5] and the Risk IT Practitioner Guide [15] was chosen as the second approach because it is an established approach to risk assessment that the practitioners of this thesis are familiar with, and is an effective approach regarding time use. This framework is also easy to follow, and it seems possible to adapt for purpose of detecting privacy risks in IdMS. The Risk IT Practitioner Guide complements the Risk IT Framework, and provides examples of how the concepts from the framework can be realized. It is an established approach developed by ISACA, based on ValIT and CobIT. The Risk IT framework has not been specificly developed to detect risks to privacy like PIA, but the risk analysis in case study 2 has been scoped to address only privacy risks and to disregard other risks.

The risk universe in Risk IT is equal to a scenario description. The framework provides certain guidelines for constructing the risk universe, and the risk universe is used to define the scope of the risk management process. The risk universe should be constructed as a workable segmentation of the system. This means that the risk universe should represent the IT applications and infrastructure that support the business objectives, processes and their dependencies. The risk universe should also contain the full value chain(s) of the organization.
Risk appetite and tolerance should also be included, risk appetite is defined as [15]: "The broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission."

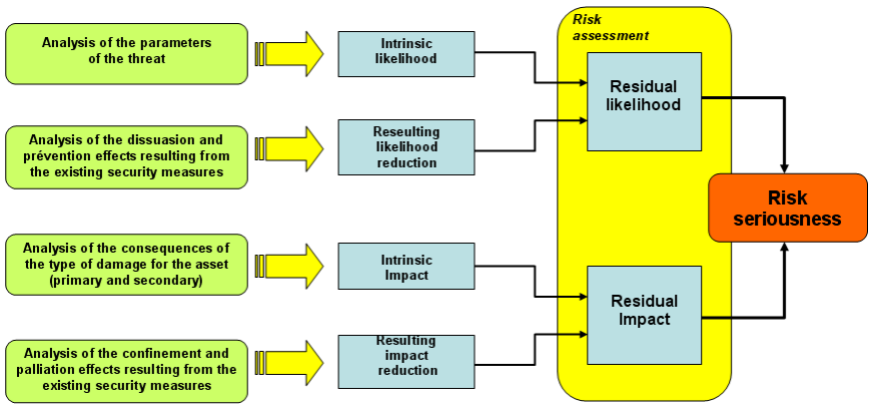


Figure 14: MEHARI Risk Seriousness. *(Source: MEHARI [14])*

While risk tolerance is defined as [15]: "The acceptable variation relative to the achievement of an objective (and is best measured in the same units as those used to measure the related objective)."
Risk tolerance is also explained as [15]:"... the tolerable deviation from the level set by the risk appetite definition, e.g., standards require projects to be completed within the estimated budgets and time, but overruns of 10 percent of budget or 20 percent of time are tolerated." Which is used in the risk assessment process to determine how much risk an organization is willing to take.

The risk analysis process of Risk IT can be seen in figure 15. To begin the process, the practitioners chooses either bottom up and top down scenario identification. The main difference here, is that top down uses the business objectives to identify risk scenarios, while bottom up is a brainstorming exercise on everything that can go wrong. A top down approach was chosen for this project, but not using generic risk scenarios as proposed by the Risk IT Framework. Since the risk identification process in case study 2 was conducted after case study 1, the practitioners felt that the brainstorming process would be heavily influenced by the already known privacy risks in the system, and a more objective approach was needed. Data flow diagrams (threat modeling) was chosen for threat identification because of the practitioners' familiarity with this approach, and because it gives an objective view of the system processes. Each identified risk scenario was refined and adapted using the attributes shown in figure 16. Since the theme of this thesis is privacy, the asset at risk was the customer in every scenario. The actors in this approach, was either categorized as internal or external agents. The "time" attribute was removed, because of the difficulties in predicting time of occurance, detection and duration without knowledge of MinID's detection systems.
The remaining attributes were used as recommended, and the "Privacy Threat" attribute was added. This attribute was used to classify the risk scenarios within the privacy risks in IdMS presented in section 5, and for comparison of findings with PIA. "Frequency" and "Impact" were the measures used to estimate the severity of the risk scenario. Frequency is a measurement of

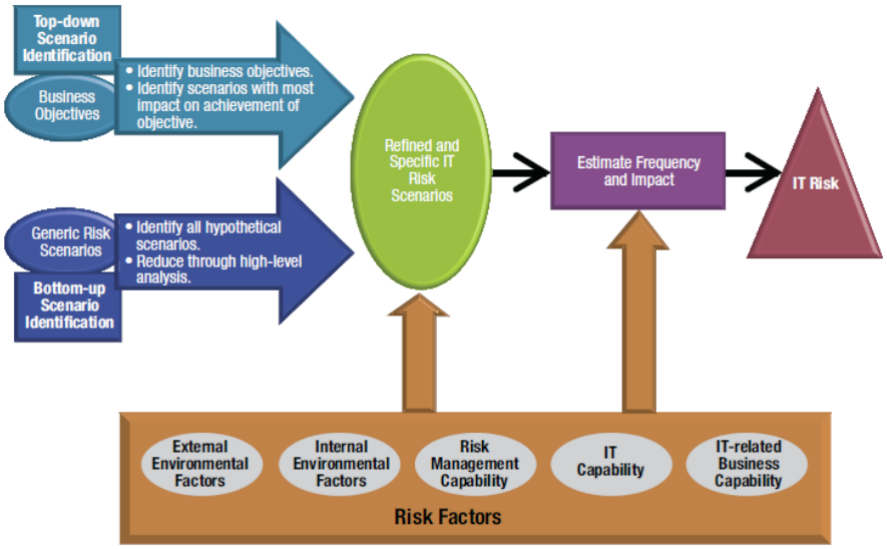


Figure 15: Risk IT Risk Identification and Analysis. *(Source: Risk IT [15])*

how often a event occurs, given values between 1-10. Impact is used to determine how severe the impact will be for the organization.

4.3.1 Threat Modeling

Scientific Modeling is the process of generating a model to help solve a problem. The models are mainly used to model either phenomena, data and theory [39]. As this method investigates a particular phenomenon, it is mostly a qualitative approach. The problems with such models is that they are dependent on the data of which the results are being computed. The advantage of models is that they allow for testing of theories while limiting the number of variables. But the flip-side to this advantage is that models do not represent all possible cases.

The systematic method used for threat discovery was data flow diagrams process modeling, also known as threat modeling when used in information security. This method was chosen because of the difference in approach to discover privacy threats, when compared to stakeholder analysis. This method maps dataflows, both externally and internally, going between processes, stores and actors. The method provides a detailed view of process flows within the organization. Breaches of every dataflow is considered using the business objectives from information security, confidentiality (C), integrity (I) and availability (A). The knowledge gained from this method will help to identify threats and vulnerabilities to the processes in the organization. An explanation of threat models:

- Processes - illustrated as a yellow circles - where activities are carried out.

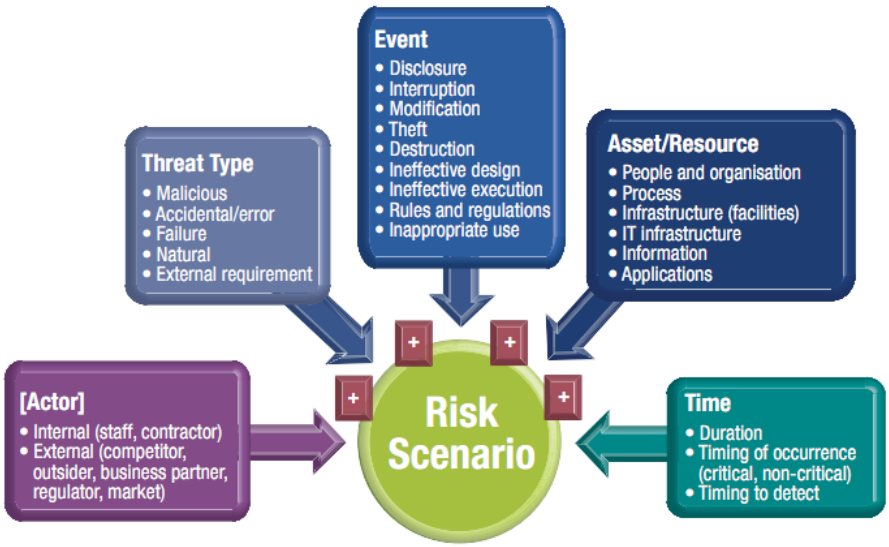


Figure 16: Components of a Risk Scenario *(Source: Risk IT [15])*

- Flows - illustrated as arrows - Input/output, what is needed for the process to carry out its activities and what the output is.
- Store/repository - illustrated as gray squares.
- Terminator (Actors) - illustrated as blue squares - external entities, outside of system interest.

An adaptation was made regarding the threat modeling, as the amount of threats discovered using threat modeling can be large (3 threats per dataflow). A critera was added to the process, where the practitioners could evaluate each risk, and if it represented any immediate threat to privacy this criteria could be answered "Yes" and qualified for further analysis. If this critera is answered "no", the threat was to be left out of further analysis.

4.4 Privacy Risk Impact for Case Studies

According to PIA [4], privacy risks fall into two categories, either risks to the individual or risks to the organization. Risks to the individual constitute harmful events that can happen to an individual in relation to privacy. And risks to the organization constitute harm that can be inflicted on an organization regarding privacy, such as a failure to meet public expectation on the protection of personal data, or the financial costs of not being compliant with law and regulations.
In this thesis the first category of these two approaches is chosen. Since this is a risk analysis for privacy, and privacy is a property of individuals, determining impact to the individual and not organizations seems only fair. Solove and PIA maps the different risks to privacy, but does not address the impact of each risk to individuals in a measurable scale.

The questionnaire is to be developed using one question per privacy risks. Developing a specific question for each threat scenario identified in the two case studies would have yielded a large questionnaire, and reduced the probability of getting answers. A possible solution for this problem when conducting a PIA or another privacy risk analysis for a company, is to create a questionnaire based on all identified risk scenarios and send it to the customers of the organization. And a practitioner in industry would be likely to only conduct one such assessment, and be able to limit the amount of risk scenarios to a manageable set. A scale of 1-10 was used as rating for each scenario, where 1 indicated "not bothered at all" and 10 indicated "severely bothered". The scale was also used to make the results transferable to the risk analysis, where the results are displayed on an equal scale.
The goal was 50 respondents and the target group for the survey was the general population. It was decided that 50 respondents or more would provide an initial insight into how the "worst case" privacy risks impact the population. Since privacy risks affects everyone, everyone was allowed to answer the survey. Using social networks and e-mail to spread the survey is an effective and quick way to distribute the survey and reach a large amount of people. But there is a risk of just reaching out to one part of the population, i.e. those not using internet daily will not be reached, this group is likely to be underrepresented in the results using this approach. The results from the survey will because of this only be used as an indicator of privacy risk impact. A more exstensive survey for mapping privacy risk impact to individuals is suggested as future work.

4.5 Summary of Conclusions

The following methodologies were decided for the solving the research questions:

- The Norwegian IdMS MinID by Difi was chosen for scenario description. This system is based on state of the art approaches to IdMS, and qualifies as a "True SSO". Documentation about the system is available in the public domain as Difi is bound by law to provide it.
- The PIA stakeholder identification is to be based on the McManus approach [30].
- The foundation of the PIA stakeholder analysis was based on Schmeer [41] and McManus [30] approaches, but the discovered stakeholder analysis approaches in related work were not found sufficient for using stakeholder analysis as a privacy threat identification tool. It was therefore decided to further develop the stakeholder analysis.
- MEHARI was chosen as risk analysis tool for PIA.
- Threat modeling was chosen as a privacy threat identification tool for Risk IT, because the brainstorming exercises and generic risk scenarios would be heavily influenced after having conducted the PIA.
- Online survey was chosen as method for determining privacy impact to individuals. The result from this survey was to be used as privacy impact in both case studies. The target number of respondents was 50, and the survey was distributed using social networks and e-mail.

5 Privacy Risks for Risk Analysis

In this chapter the privacy risks used for both risk analyses are explained, outlined and explained based on previous work. The privacy risk classes defined in this chapter are based on previous work by Solove [6] and the Privacy Impact Assessment [4]. This process resulted in 5 main classes and 19 individual classes for privacy risks. These risk classifications are used in the risk analysis of both case studies within this thesis. The impact values for the 19 privacy risk classes are also determined within this chapter.

5.1 Privacy Risks for IdMS

Having defined the term privacy in section 2.1, privacy risks can be addressed. What can threaten to invade privacy? And what are common threat factors that can put privacy under pressure?
In 2006, Daniel J. Solove [6] published a taxonomy of privacy. This article identifies in total sixteen different classes of threats to privacy (all of which are illustrated in figure 2). Many of the risks provided by PIA are similar to the definitions provided by Solove, but the risks provided by PIA have been provided for detection purposes, and is therefore from another point of view, adding three additional risks to the taxonomy. The following is an explanation of Solove's taxonomy and the additional PIA risks, it is divided into five main categories and their corresponding sub-categories of threats.

- **Information Collection:** Is a risk classification where information is collected about an individual. There is two categories of information collection risks:
  1. Surveillance: Is any type of surveillance where information about natural persons can be gathered, such as visual surveillance, audio surveillance and recording of activities. These technologies can be used to listen in on peoples' telephone calls and conversations, and to gather information on dealings between two people or identify them in locations to track movement. Surveillance can be used as a means of controlling human behavior [50] and be used as a tool for social control [51]. One of the examples provided by Solove is using surveillance as a deterrent from committing crime.
  2. Interrogation: According to Solove interrogation is "... the pressuring of individuals to divulge information", through questioning and probing. A thought that might occur in the mind of the reader, is that interrogation only occurs when citizens are suspected of committing crimes (or something similar) and is called in to an interrogation. But this

is not the case, citizens are being interrogated through questionnaires, registration forms and interviews. I.e. The fear of not getting a job during a job interview, can be enough of pressure on an individual to part with personal information he or she would rather have kept secret.

- **Information Processing:** Solove defines this category as the way information is stored, manipulated and used. This category is not concerned with the gathering of data, but it is concerned with handling of data that is already stored.
  1. Aggregation: Aggregation is combining various sources of information to reveal information about the user that he thought was hidden. This is an invasion of privacy because we as users expect boundaries on what is know about us, and what is not, this technique crosses these boundaries. Such as the local tax department discovering that what was written as a business trip was really a vacation trip, through accessing multiple sources of information.
  2. Identification: is linking collected information to particular individuals. Such as linking information about previous illnesses and medical conditions to fully functional and recovered individuals.
  3. Insecurity: is improper storing of personal information, which leads to leaks and improper access. Insecurity can lead to incidents such as identity theft.
  4. Secondary use: is the use of information collected for one purpose for a different purpose without the data subject's consent. Such as using information collected in a fingerprint experiment to identify individuals at a crime scene.
  5. Exclusion: Concerns storage of personal data without letting the data subject know about it, and excluding the data subject from access ti the data.
- **Information Dissemination:** all these threats involve spreading or transfer of personal data or the threat to do so.
  1. Breach of Confidentiality: Is breaking the promise to keep information confidential. Such as breaking a duty bound voe of silence, and leaking confidential information about an individual.
  2. Disclosure: Is revealing truthful information about a person that can harm the him/her. Such as revealing a hidden address of a person under a witness protection program.
  3. Exposure: Involves exposure of another person's nudity, grief or bodily functions. This is a common risk in todays social networking society, i.e. posting exposing pictures of other people on the Internet.
  4. Increased accessibility: is amplifying the accessibility of information. Such as combining several publicly available data records to create a customer profile.
  5. Blackmail: Is threatening to disclose personal information about an individual to force the individual to do something they otherwise would not.

6. Appropriation: Involves using a person's identity to serve some purpose against their will or without their knowledge. Such as using the picture of a person in marketing campaign without his/hers consent.
7. Distortion: Is the activity of obfuscating and distorting information about a person, making the information erroneous and misleading. Such political campaigns where smearing the candidate's name is the main purpose, to draw negative attention to his/her person.

- **Invasions:** This class involves invasions into people's privacy, and does not necessarily include the handling of personal data.
  1. Intrusion: Defines acts that invade or intrude other persons tranquility or solitude. Such paparazzi photographing of celebrities.
  2. Decisional Interference: Is when an authority invades on peoples' ability to make choices on their own. Such as banning the use of tobacco from pubs and bars.
- **PIA risks:** These are risks that are added to the taxonomy by literature present in the Privacy Impact Assessment Handbook v2.0.
  1. Denial of Anonymity: Is the activity of identifying individuals where it is unnecessary to do so. Such as using an identifier that can be traced back to one particular user.
  2. Function Creep: Is the increase of scope when using personal data. Such as using the social security number, which was designed to be used for tax purposes in the 1960s, for logging into MinID 50 years later.
  3. Legal Considerations: Is when a data handler is not being compliant with laws and regulations regarding handling of personal data.

5.2 Determining Privacy Risk Impact

To be able to measure impact, survey was chosen as a method. A survey is a quantitative approach for gathering data [38]. The survey (questionnaire) was designed to aid the work of determining how much a privacy risk can impact a person. The questionnaire was founded on the privacy risks presented in the previous section. The questionnaire was based on worst case scenarios of risks materializing. One scenario per risk was used to give an indication of the impact of each risk to individuals. More scenarios could have been developed for each risk to obtain a more accurate result, but due to time limitations, a larger and more complex questionnaire could not be processed. Due to time limitations the decision was made to create one questionnaire to create a foundation for assessing impact to privacy.

The questionnaire was sent to a group of three students for feedback and quality assurance before being published on the Internet. This was a "worst-case scenario" approach and the results were expected to be weighted between 5 and 10 for most of the risks. The questionnaire was open for only one day, and received 68 replies during that time frame. The results from the questionnaire

can be seen in table 17 and is illustrated in figure 18. The complete survey can be found in appendix E.

Privacy Risk Impact assessment		
Privacy Risk	**Mean value**	**Privacy Impact**
1. Surveillance	7,7	Very High
2.Interrogation	6,6	High
3. Aggregation	6,5	High
4. Identification	8,2	Very High
5. Insecurity	8,6	Very High
6. Secondary use	7,8	Very High
7. Exclusion	8	Very High
8. Breach of Confidentiality	8,4	Very High
9. Disclosure	8,3	Very High
10. Exposure	7,8	Very High
11. Increased Accessibility	6,6	High
12. Blackmail	8,3	Very High
13. Appropriation	7	High
14. Distortion	7,5	Very High
15. Intrusion	6,4	High
16. Decisional Interferens	6,2	High
17. Denial of Anonymity	6,9	High
18. Function Creep	7,9	Very High
19. Legal Consideration	7,8	Very High

Figure 17: Privacy Risk Impact with results from survey.

The risks and their worst-case privacy impact is illustrated in figure 18. No low (green) and medium (yellow) risks were present in the results of the questionnaire, all the privacy risks used in this thesis were between 6.2 to 8.6. High is illustrated as orange, and very high is illustrated as red.

5.3 Summary of results

The combination of Solove's taxonomy [6] and PIA privacy risks [4] resulted in 19 individual privacy risk classes to look for. Each of these risks were addressed with one worst case scenario in an online survey. The purpose of this survey was to obtain a measure of impact for the two case

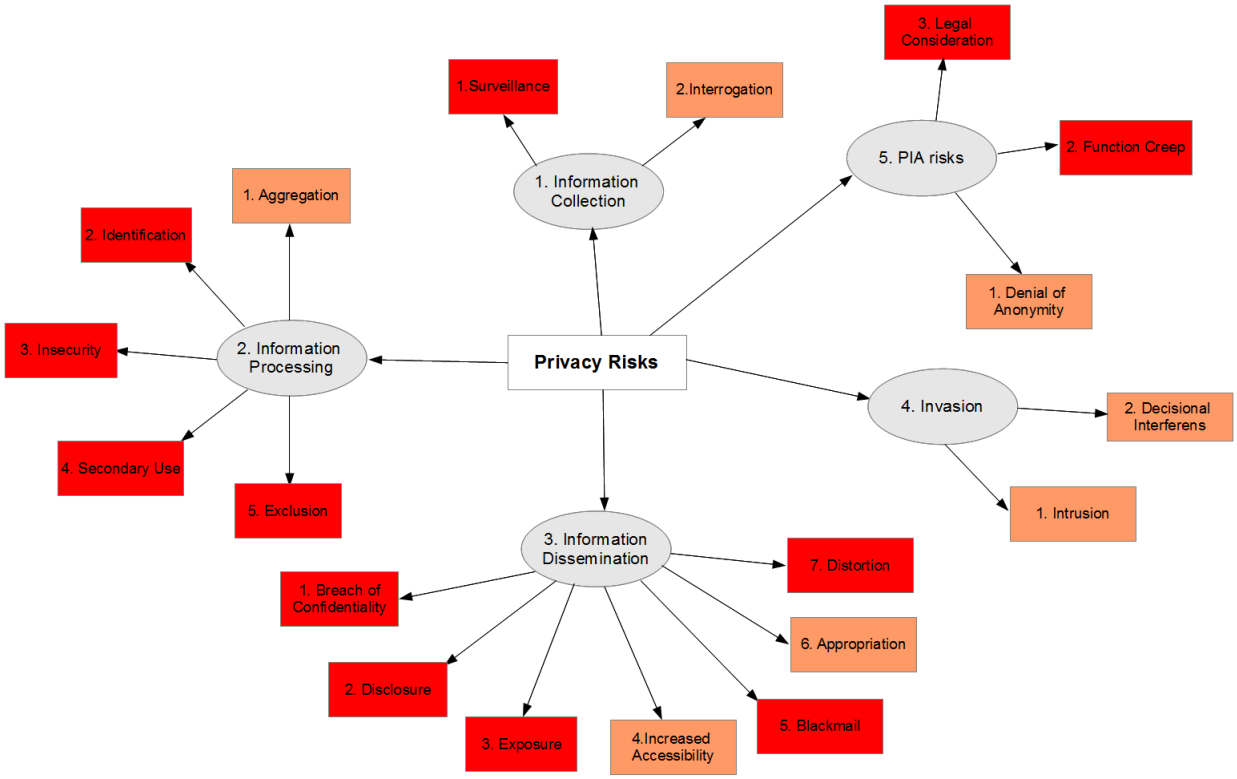


Figure 18: Illustration of the Privacy Risks addressed in this thesis

studies. The goal of 50 respondents was reached in 24 hours, and the survey was closed after a day having obtained 68 respondents. Since the survey was worst case, the gathered results were, as expected, weighted between 5-10 ("High" and "Very High" impact). Results are illustrated in figures 18 and 17.

6 Stakeholder Analysis as Privacy Threat Identification

Recall in chapter 4, that the methodology for stakeholder identification in this thesis was based on the approach by McManus [30]. The foundation of the stakeholder analysis to be conducted in case study 1 was based on the Schmeer [41] and McManus [30] approaches, but the discovered stakeholder analysis approaches in related work were not found sufficient for using as stakeholder analysis as a privacy threat identification tool. This chapter presents an expansion of the stakeholder analysis methodology from chapter 4, developed for this thesis with the purpose of detecting privacy risks in IdMS. An approach to using stakeholder relationships and assets to help determine likelihood adapted to MEHARI [14] risk analysis is also presented.

6.1 Expanded Stakeholder Analysis

The complete stakeholder analysis can be found in appendix D. This section contains a complete explanation of each stakeholder attribute chosen for the stakeholder analysis, and how they are used in case study 1 for threat identification and calculation of probability.

Influence and importance to project (IdMS)

The values high, medium and low was used to determine *influence and importance* in the project. This was also used to determine which stakeholders to include and exclude. For influence these three categories were defined as:

- High - can cause major changes in MinID. Such as new laws, regulations and policies, or in charge of money flows. Can also influence high level system architecture and attributes.
- Medium - can influence changes in MinID, but only to some extend. Stakeholder can influence changes in software, functionalities, and similar low level attributes. Can influence money distribution, but not final decision maker.
- Low - some or none influence in MinID. Stakeholder can suggest changes, but has no real power to influence changes.

And for importance these three categories were defined as:

- High - Major considerations must be given this stakeholder in MinID. Such as if MinID is

bound by laws or regulations to prioritize the stakeholder, or if the project lifetime is dependent on the stakeholder for future survival.

- Medium - Medium considerations in MinID, such stakeholders that need ethical considerations.
- Low - Some or no considerations in MinID, should be considered, but does not need to have any importance to the solutions presented in MinID.

6.1.1 Capabilities

A capability is an ability to perform, such as choosing to use a system, or choosing to attack a system. The capabilities of the stakeholder are essential in this stakeholder analysis, as it is the consequences of these capabilities that will be analyzed.
Each stakeholder in our analysis has a set of capabilities, this set was non-exhaustive. An effort was made to narrow them down to the capabilities that could potentially affect privacy. The capabilities analyzed was by no means the only capabilities the stakeholder had concerning privacy, but given the time limitations of this project, the capabilities were reduced to a manageable set. Privacy and personal data were keywords in this process, the capabilities that were not estimated to have any affect on these two were left out of the analysis. Both the assets and capabilities can be mapped through interviewing (see Schmeer's approach [41] for guidance), this analysis is based on open sources and the capabilities were assigned to the stakeholders using available literature about the system (see chapter 7 for more information).

6.1.2 Incentives

An incentive is something that motivates an actor to act on a capability. It can be used to determine why an actor chooses to do something. An example is a criminal who chooses to rob a bank, where the incentive is financial, to obtain money.
The book "Halting the Hacker: A Practical Guide to Computer Security" [52] contains a taxonomy of incentives for an attacker. The incentives used from the book are: "military, political, business, financial, advertisement, terrorism, grudging, self assertion, fun". Audestad [53] also addresses these incentives. "Carelessness" was added to the matrix as this can also trigger risks to privacy. There may also exist other incentives, but these were left out of the taxonomy. In this analysis, the incentives of each stakeholder is used to determine the value of each asset. Based on the definitions provided in the literature by Pipkin [52] and Audestad [53], the terms in this thesis have been defined as::

- Military - military gains, such as demoralize the population, disseminate propaganda, destabilize a country, gather intelligence, or take down or disturb the operation of certain infrastructures.

- Political - Political gains, such as obtaining political support, obtaining more funding through politics, obtaining political advantage, etc...
- Business - Strengthen business processes, gain more subscribers, steal information, gather intelligence concerning business processes, obtain competitive advantages, get rid of competitors, etc...
- Financial - gain financial advantages, obtain more funding, steal money, bonds and securities, personal gains, etc...
- Advertisement - Spread advertisement in order to reach a large audience and increase customer base or spam.
- Terrorism - Damage the system, cause havoc, vandalism, etc...
- Grudging - Revenging some real or imaginary injustice.
- Self-assertion - Demonstrating dexterity with computers and knowledge of how to penetrate a system for acknowledgment, or promoting one self i.e. for promotions or increase in salary.
- Fun - People not comprehending the effects of playing with the computer and the network may do something dangerous just by chance - or as the famous theoretical physicist and Nobel laureate Richard Feynman has put it concerning experimentalists, "If you do enough experiments, it is not unlikely that you come up with something interesting."
- Carelessness - Neglecting to follow policy and rules when using the system, because of staff burn out, tired of job, etc...

6.1.3 Attitude and Knowledge

The majority of tools that were evaluated for conducting the stakeholder analysis (see [31, 41, 54]) recommends determining the attitude of the stakeholder towards the project. This is added as a means to determine who is likely to mobilize for or against what is intended, as recommended by McManus [30]. Attitude is also used to determine allies and opponents in the stakeholder analysis.
The knowledge level of each stakeholder is related to their own capabilities, are they aware of their own potential to influence assets and other stakeholders through their own actions? Or are they unaware of their own importance and capabilities in the system. This is important when considering future consequences of potential actions and likelihood of consequences (positive or negative) materializing. Knowledge level is in case study 1 used to help determine probability of the stakeholder acting upon his capabilities.

6.1.4 Assets

Assets are defined by Swiderski and Snyder [35] as: "An abstract or concrete resource that a system must protect from misuse by an adversary". The terms that are used in this project are

intangible (abstract) and tangible (concrete). The main goal of the intangible asset in the stakeholder analysis was to cover the important intangible assets in relation to privacy. These assets are present in the system or among the stakeholders, and have the potential to cause privacy risks. The paper published by Johnson [55] in 1999, was used as a guidance for compiling an initial list of intangible assets. This list was used as guidance when discovering intangibles for each stakeholder.
All the identified assets have relations to the capability of stakeholders. Stakeholder assets without any relation to capabilities have been left out of the analysis.
Estimating the value of an intangible asset is not a straight forward job, this is because the same intangible asset may have different value when assessed by two different persons. What is meant here is that the values of intangible assets varies from individual to individual. I.e. some individuals would sell their sensitive personal data for a prize, but the amount of money may vary. One person might sell his personal data for 100.000 NOK, while another person sells for 1.000.000 NOK. It is therefore hard to determine value of an intagible asset for a particular stakeholder without direct interviews. Because of this, it was decided to assign both ingatible and tangible assets using high, medium and low to indicate the relative value for the stakeholder, instead of assigning a numerical value.

- High - Assets in direct relation to incentives of the stakeholder.
- Medium - Assets moderately related to incentives of the stakeholder.
- Low - Assets has weak relations to the incentives of the stakeholder.

The evaluation is based on the incentives of the stakeholder, the incentives have high priority, and all assets directly related to an incentive will therefore have a high priority. Assigning erroneous values to the assets may lead to a false conclusion when assessing capabilities of each stakeholder and the likelihood of stakeholders acting on these. A point in this thesis is that the stakeholder analysis conducted in the case is based on a "best effort", and evaluation of assets are estimated by the authors. Quality assurance of the analysis methodology is suggested as future work.

6.1.5 Relationship with other Stakeholders

Determining relationship between stakeholders is based on the research results when designing the scenario. The relationships were divided into allies, neutral and opponents. This was done to help determine likelihood of a stakeholder acting on his capability. In this project the stakeholders have simply been divided into categories, but as a suggestion for a more detailed and reliable stakeholder analysis, the practitioner can assign utility values to the relationships between each stakeholder.
The relationships between stakeholders was used to help determine probability of a stakeholder acting on a capability. If the capability affects another stakeholder negatively, the stakeholder is less likely to act upon his capability.

6.1.6 Consequences of capabilities on assets and affected Stakeholders

This is the part of the analysis where potential risks to privacy can be detected. Each capability from the set is analyzed in this stage of the analysis. The 4 categories used in this analysis was capability, assets affected, effect (for stakeholder) and affected stakeholders. Capabilities that were similar, or with similar consequences was grouped together to limit the complexity. The "Asset(s) Affected"-column represents the stakeholder's assets, and the impact of the capability on these assets. The impact is denoted with either a positive (+) or a negative (-) impact.
The effect column contains a short written description of how the capability affects the stakeholder, assets, system and other stakeholders. While affected stakeholders are denoted with either a positive (+) or a negative (-) impact. An example of an application of this method is illustrated in figure 19, the figure shows an analysis of a capability that Difi has.

Scenario nr	ACTOR	CAPABILITY	ASSET(s) AFFECTED (Positive or negative)	EFFECT *(for stakeholder)*	AFFECTED STAKEHOLDERS (Positive or negative)
4	1.3 Malicious Insider and Non-compliant employees	Selling information	- MinID database (-) - User subscription list (-) - MinID User logs (-) - System Documentation (-) - System Security Information (-) - Subscriber privacy (-) - Cash (+) - Anonymity (-)	- Obtain information about *User(s)* and *Internal actors (Difi)* - Lose Anonymity - Gain cash by selling information	- User (-) - Interal actors (-) - Competitors (+) - Attackers (+)

Figure 19: Example of Consequence of capabilities

Each stakeholder has a set of capabilities and assets (for more information, see appendix D). When acted upon, the capability affects the assets of the stakeholder, and other stakeholders and their assets as well. A graphical illustration of the threat scenario in figure 19 is seen in figure 20. An explanation of the figure 20: The actor in this illustration is the malicious insider (and non-compliant employee). He wants to sell personal information acquired illegally in the system, which is the capability (illustrated as oval). Affected assets are illustrated in rectangles. The consequences, either positive or negative, are illustrated with plus (+) or minus (-). As can be seen from the figure, this capability affects the privacy of the users negatively, and the actor risks his anonymity while gaining cash. While the capability also affects other stakeholders and their assets in various (and maybe unforeseen) ways.
The purpose of this analysis is to find capabilities that affect the asset "Subscriber privacy" negatively. When the privacy asset is affected negatively, a threat has been discovered. And the practitioner can use the threat to create a risk scenario for further analysis.

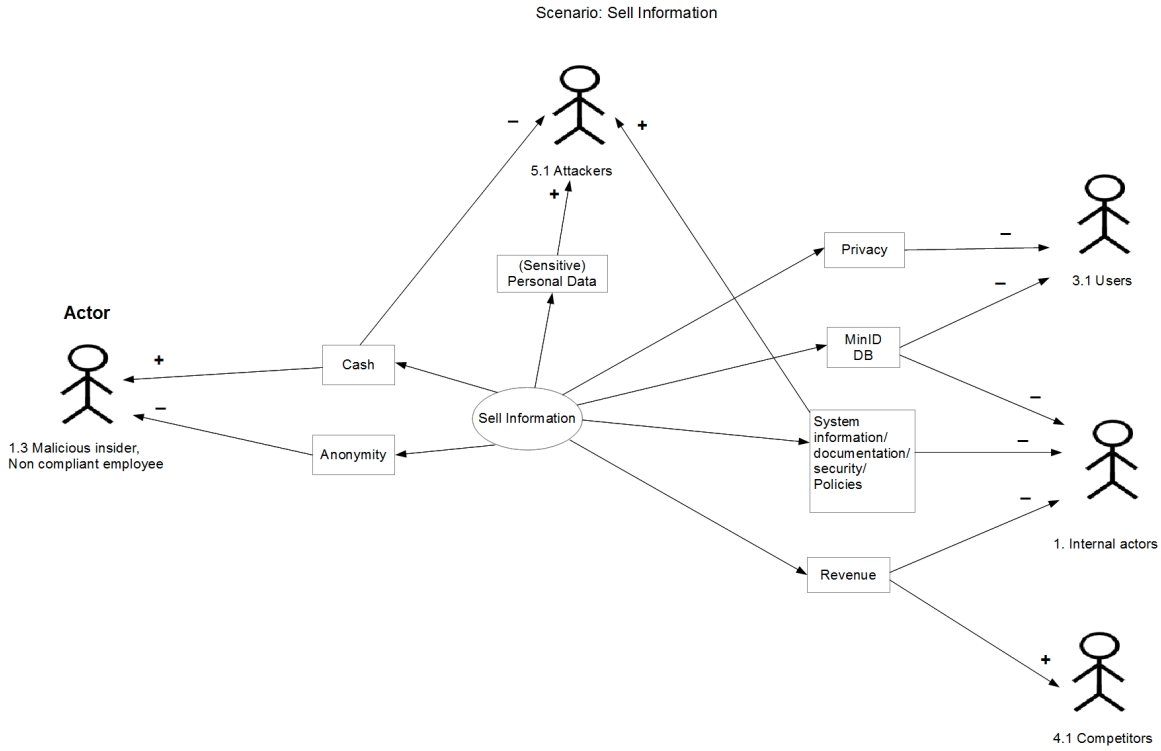


Figure 20: Stakeholder capability.

6.2 Using Stakeholder Attributes to help determine likelihood

In this section an example is provided of how the attributes from stakeholder analysis (see appendix D) can be used to help calculate risk likelihood. This example uses the probability scheme from MEHARI [14], which uses residual likelihood and residual impact to calculate "Risk Seriousness".

Determining preferences for a stakeholder without direct interaction is likely to give erroneous results. The risk analysis is therefore used as an example of an approach on how the practitioner can utilize the attributes from the stakeholder analysis to estimate risks to privacy. The authors of this thesis is aware that the presumption that every stakeholder can be considered rational is a big one, and that assigning a preference value to an asset or a relationship comes with high degree of uncertainty. But as this thesis is more about methodology for privacy risk analysis, than the actual results of the risk analysis, the liberty has been taken to assign subjective values to such relationships by the practitioners. This is to illustrate how it can be done using a stakeholder approach.
There is also room for arguing that counting goodwill and reputation as assets is redundant when the relationship between stakeholders are considered as a separate process. This was done be-

cause goodwill and reputation might affect relationships with other parties than the stakeholders considered in this analysis, and can, according to Johnson [55], be considered an asset in itself.

To help determine likelihood, the different attributes from the stakeholder analysis were assigned the following preferences:

- Knowledge level: is used to determine likelihood of a threat scenario occurring, in this thesis three different levels of knowledge were used. A value of likelihood used to help calculate probability, illustrated in figure 21 knowledge level table.
- Asset evaluation: illustrates how much the stakeholder values an asset. There has been assigned numerical preferences to asset evaluation. These values are illustrated in asset evaluation table in figure 21. The asset evaluation are used in probability calculation, and affects the decisions of the stakeholder.
- Actions affecting relationships: the matrix, action evaluation in figure 21, shows the preferences of the stakeholders. If a capability negatively impacts allies, this is used as an argument for not acting upon the capability.

All the numbers in table 21 are numbers assigned by the practitioners in case study 1. Interviews with each stakeholder can be used to assign more correct numbers. The scales in the figure are the same for each stakeholder in this analysis to help reduce complexity of calculations.

Level	O( )
3	0,6
2	0,4
1	0,2

knowledge level

Value	P( )
High	0,15
Medium	0,1
Low	0,05

asset evaluation

	ALLIES	NEUTRAL	OPPONENTS
Positive	0,1	0,05	-0,1
Negative	-0,1	-0,05	0,1

action evaluation **(Q)**

Figure 21: Weighted Attributes

The likelihood calculation is based on data from the scenario and stakeholder analysis, adapted from MEHARI. Following is an explanation of the calculations of likelihood:

- Intrinsic likelihood = (Knowledge level + Assets Rewarded + Relationships rewarded)

- Control efficiency = (Assets Risked + Relationships Risked)
- Residual Likelihood = (Intrinsic Likelihood - Control efficiency)

An example of the calculation of likelihood can be seen in figure 22, additional information has been added to each column to help explain each calculation. Each of the preferences in figure 21 are found in the the calculation.

Scenario nr	Actor	Knowledge level (O)	Assets rewarded (P1+Pn)	Assets Risked (P1+Pn)	Relationship rewarded (P1+Pn)
1	Difi Management	0,6	0,15+0,15	0,10+0,10+0,10	(-0,10)+(-0,10)
2	Difi Departments	0,6	0,15+0,10	0,15	0,10+(-0,10)+(-0,10)
3	Difi Departments	0,6	0,15+0,15	0,15	-0,1

Scenario nr	Relationships risked (Q1+Qn)	Intrisic likelihood (Knowledge level + Assets rewarded +Relationships rewarded) <1&>0	Control effiency (Asset risked + Relationships risked)	Residual Likelihood (Intrisic likelyhood – Control efficiency 1)
1	0,05	0,7	0,35	**0,35**
2	0,05+(-0,10)+0,10	0,5	0,2	**0,3**
3	0,05	0,8	0,2	**0,6**

Figure 22: Example of Likelihood calculation

6.3 Summary

In this chapter, an attempt has been made to scope stakeholder analysis for detecting privacy risks, together with a suggestion for using stakeholder attributes to help determine likelihood with MEHARI [14]. The stakeholder analysis consists of:

- Influence and importance - reflects the stakeholders position in the project.
- Capabilities - reflects what actions the stakeholder can perform that affects the project, assets and/or other stakeholders.
- Incentives - the classifications of incentives are adapted from literature by Pipkin [52] and Audestad [53].
- Attitude and Knowledge - reflects if the stakeholder is likely to mobilize for or against the project, and awareness of his own potential to influence assets and stakeholders through their own actions.
- Assets - "An abstract or concrete resource that a system must protect from misuse by an adversary [35]." Asset has some relation to privacy or personal data.
- Relationship with other Stakeholders - stakeholder allies, neutral and opponents.
- Consequences of capabilities on assets and affected Stakeholders - describes how the capabilities of one stakeholder may affect his own assets and relationships with other stakeholders.

7 Scenario Description

This Chapter gives an introduction to the scenario used in this thesis. The full version of the scenario, including a full presentation of all the stakeholders, can be found in Appendix C.
The case study in this project is based on the MinID identity management system provided by the Norwegian Agency for Public Management and eGovernment (Difi) [3]. MinID is a part of the federation called "ID-portal" (ID-porten) which can be logged into using MinID, or other eID providers. The ID-portal facilitates access to public services like tax, health services and many others. In April 2010, the number of registered Norwegian citizens using MinID increased to over 2 million users [45].

7.1 Scenario background

Difi is an organ of the Norwegian government, and their vision is "We develop the public sector" [3]. Difi aims to contribute to the public sector by renewing and developing it, and strengthen cooperation between vendors and offer joint solutions. Their goal concerning electronic identities is to establish a joint infrastructure for use of electronic identities in government sectors [56]. To achieve this objective, they have developed the solution known as MinID. The main objective of MinID is to ensure access to governmental services through the use of electronic identities in a secure way [42].
In 2005, Difi defined specifications for establishing a public key infrastructure (PKI) in Norway, which was later approved by the Norwegian government [57]. The specifications were later updated and the newest version is from 2010 [58]. These specifications are the basis for regulation of requirements of eID and e-signature. MinID is Difi's PKI solution.
According to Jon Ølnes (lecture AF Security seminar, University in Oslo 25.01.2012), Difi views a person's electronic identity as [56]"... the collection of all electronic information that can be attributed to the person" . The scope of this scenario is privacy and the system's handling of privacy sensitive information. This scenario first provides a short description of MinID as a system, and the different functionalities of the system. The second part contains a brief introduction of MinID's stakeholders identified as a part of this project. To log in using MinID, the user applies his/hers Norwegian social security number (fødselsnummer, consists of 11 numbers) or D-number (temporary number given to foreign citizens that pay taxes to Norway) [59], a personal password and a one-time PIN code. The PIN code is either found on piece of paper containing several codes delivered by mail, or it can be sent to the user's mobile telephone if he/she has registered the telephone number. The latter is becoming the more common solution [3], as paper is regarded as an old-fashioned solution.

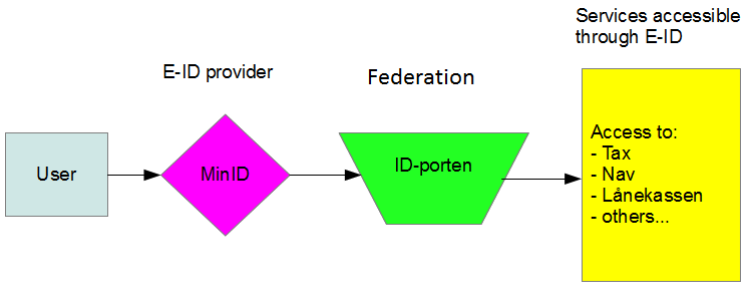


Figure 23: Illustration of how ID-porten and MinID works.

7.1.1 Difi Objectives

One of the main reasons for implementing ID-porten and MinID is the amount of time and money that can be saved through digitalizing of the public services. Other Difi goals are [56]:

- The public sector will use Difi's knowledge, means and tools, something which is achievable only through cooperation and dialog.
- Good cooperation with the rest of the government is the most important prerequisite for our success.
- Difi has a special responsibility for the renewal and development of public sector in the areas of ICT, procurement, communication, organization, instruments and training.
- Transactions between citizens and the government should mainly be digitalized.
- Digital solutions shall be offered for all suitable governmental services.
- Digital services shall be shaped by the user's need and be secure and effective.
- MinID is to be based on open source solutions.
- Handle foreign logins.

7.1.2 MinID purpose and functionalities

MinID is an identity management system that holds access credentials for Norwegian citizens, and provides authentication for accessing many services provided by the Norwegian Government, such as [60]:

- Altinn.no - site for handing in electronic schemes for public services.
- brreg.no - National registers in Bronnoysund.
- lanekassen.no - Unit for financial support for students.

- NAV.no - The Norwegian Labor and Welfare Administration.

The illustration shows how MinID can be used to gain access to public services through the ID-portal federation. "eID providers" can also refer to Commfides and Buypass (or others) developed solutions, which are two other alternatives for logging into ID-porten. This is one of the three main tasks for which MinID can be used. According to Ølnes [56], it can also be used to *digitally sign and verify documents*, and to *facilitate encryption and decryption*. These two functionalities, together with handling foreign logins, are out of scope for this thesis.

7.2 The MinID IdMS

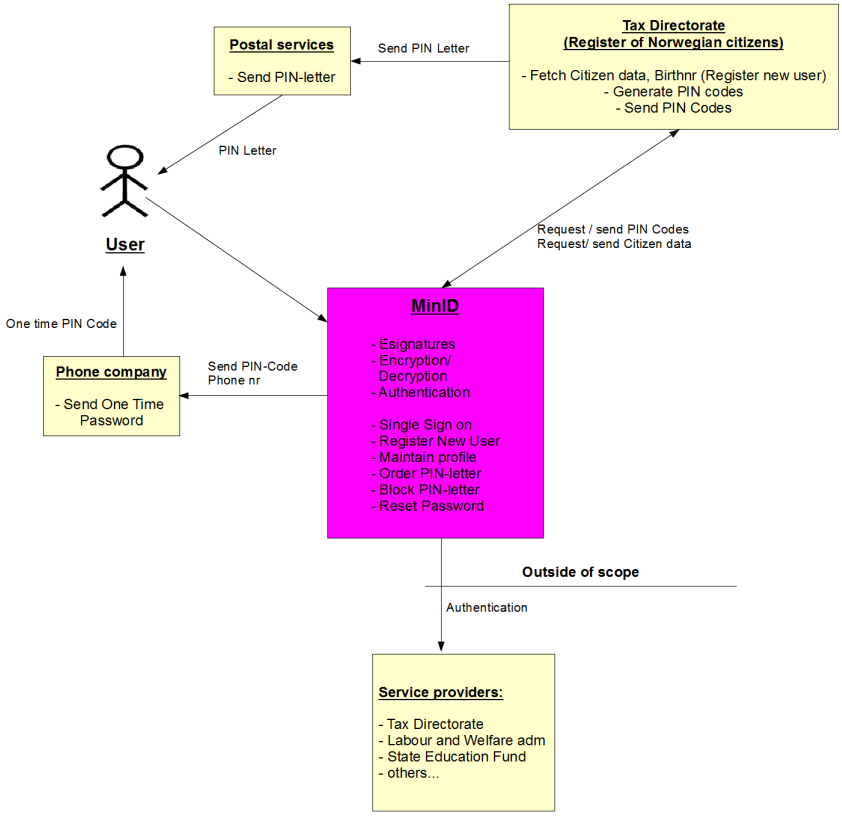


Figure 24: MinID IdMS

The view of the system that was used in this case contains a distinction between the information actually present in the MinID IdMS, and the information it provides access to. The system is illustrated in a top-down view in figure 24. The figure represents the different parties directly involved with MinID. The purple rectangle in the middle represent the main services offered by MinID. And the pale yellow rectangles are service providers directly in contact with the MinID

system. The encryption/decryption and eSignature functions are not considered as a part of the scope in this project. A short explanation of the figure:
The purple rectangle in the middle includes the services provided by MinID. MinID has several contact points, the User (represented by the stick man) can use the services provided by MinID. If the user authenticates through MinID to use any public services, the personal data accessed after entering the website of the service provider (Tax, NAV, etc...) is outside of the scope of this case study. This was because of the privacy statement published earlier by Difi [61] which states that the public services are responsible for the personal data in their own systems. The Tax directorate holds citizen data about all Norwegian citizens with a social security number, and is in direct contact with MinID when new users are registered [61]. The tax directorate is also the handler of PIN letters [62], these are ordered on the MinID portal provided by Difi. MinID sends one time PIN code through the Phone Company back to the user's registered mobile telephone number.
The system depicted in figure 24 is illustrated according to descriptions gathered from open sources. The personal information the system handles, are social security numbers, PIN-codes, passwords, e-mail addresses, telephone numbers and logs containing usage of MinID for each user. What has been gathered about the content of these logs is depicted in figure 25, the content illustrated has been confirmed present, but there is a possibility that the logs contain more information about the user (sources Difi website [2, 42, 62] and Appendix F). Difi is characterized as a data handler according to Norwegian law [18].

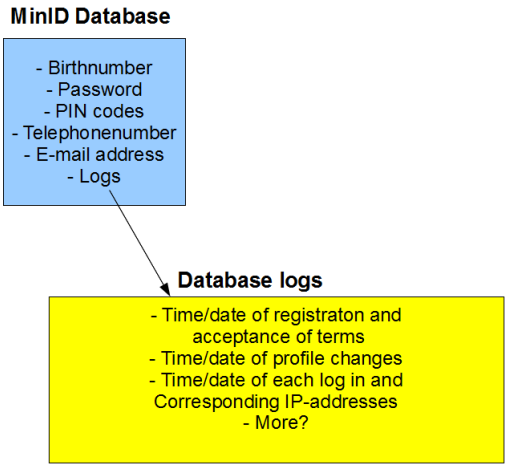


Figure 25: Personal data in high level database.

7.3 Stakeholders, MinID

There are many different stakeholders involved in MinID. To get an overview of the stakeholders related to MinID, they have been categorized using a top-down approach, illustrated in figure 26. Where class 1 is a general classification of the type of stakeholders, and class 2 is more specific.

Class 3 is not represented in the figure, but are represented in the following stakeholder analysis (colors are for illustrative purposes to indicate levels). This Chapter contains an introduction and description of the stakeholders, as well as a summary of the analysis. The complete stakeholder analysis can be found in the Appendix D.

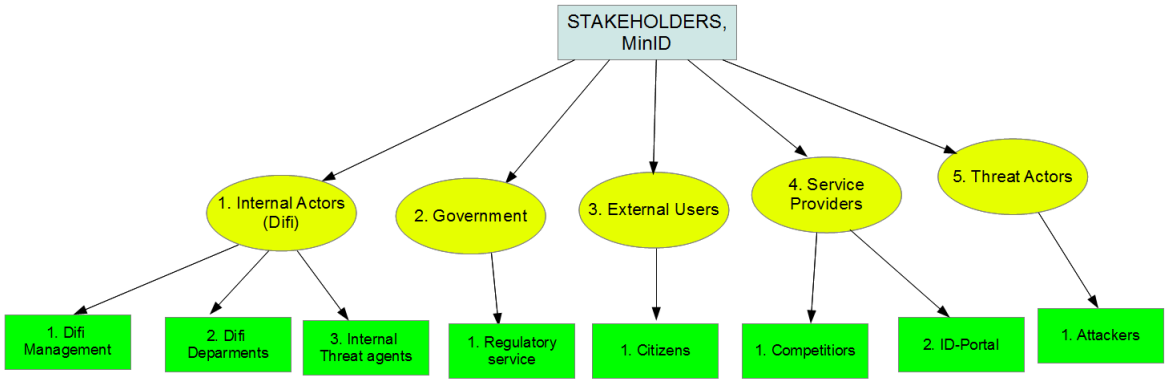


Figure 26: Categorization of stakeholders class 1 and 2.

The methodology for the stakeholder identification and basic analysis is found in section 4.2.2. Stakeholders that have been identified as important for this case are listed in this section, and their corresponding sub-categories are addressed in the list below. The number of level three stakeholders to be analyzed have been limited to eight to reduce complexity and time use of the task. See Appendix C for a complete description of each stakeholder, and Appendix D for the complete stakeholder analysis conducted as a part of this thesis.

- **Class 1 - 1.Internal actors(Difi)** - This class represents all the internal actors that are somehow connected to MinID, either through employment or other means. These actors include the Difi management, Difi departments, developers, operators, and generally all who has a stake in the project.
  1. Difi Management - Are decision makers, both for Difi as an organization and for the MinID system.
  2. Difi Departments - These are the departments that have been found to be significant, and have a direct stake and influence in the project.
  3. Internal threat agents - This class consists of the malicious insider and the non-compliant employee, and represent the human factor in information security.

- **Class 1 - 2. Government** - This class represents government stakeholders that have interaction with MinID.
  1. Regulatory services - The government bodies included in this class have a stake in MinID.

These are the Norwegian Data Inspectorate, Privacy committee (Personvernnemda) and policy, law and legislation makers.

- **Class 1 - 3. External users** - This class represents users of the MinID IdMS, which are mainly Norwegian citizens and holders of D-numbers.
  1. Users - This stakeholder group consists of Norwegian citizens and holders of D-numbers. The users are the main target group for the MinID project, and the system is scoped and developed to fit the users requirements.

- **Class 1 - 4. Service Providers** - This class represents the other service providers that can be used to access the ID-portal, and the available public services available through the ID-portal.
  1. Competitors - This stakeholder represents all other eID providers in the ID-portal.
  2. ID-portal - The ID-portal stakeholder represents all the service providers accessible through MinID. Some of these services handle sensitive personal information for each user, but this data handling is not within the scope of this case.

- **Class 5 - 1. External threats** - This class represents external threats to the system, these have been identified as (but not limited to) hackers, crackers, computer criminals, terrorists, industrial spies and automated attacks (such as worms, virus and other malware).
  1. Attackers - This stakeholder class represents the external threats to MinID.

7.4 Summary of the Scenario description

The first part of the scenario addresses the background and objectives of MinID, why it was developed, and by whom. Difi is regarded as a data handler according to Norwegian law, but is only responsible for the personal information within their system. They are not responsible for the information accessed using MinID. Two known databases are used by MinID, one that stores personal data about the users, such as social security number and e-mail address, and a high level database that stores sensitive personal data about the users, i.e. IP addresses, and time and date for logins.
The number limit of class three stakeholders was set to eight. The methodology presented in section 4.2.2 was used for stakeholder identification in this scenario.
See the Appendix C for the complete scenario description containing, among other things: an extended description of the system, existing privacy policies, laws and regulations, technologies and solutions used in MinID, and a complete presentation of the stakeholders in the system.
See the Appendix D for the complete stakeholder analysis conducted using the methodology described in Chapter 6.

8 Case study 1 - Privacy Impact Assessment

The first case study was performed using the UK Privacy Impact Assessment method published by the Information Commissioner's office. The version used in this thesis was the PIA Handbook version 2 [4], which was released in June 2009. The case study was performed on the scenario presented in the chapter 7.
This chapter contains general comments and discussion of conducting the PIA according to the framework. The initial assessment and the 4 first phases of PIA are addressed (see chapter 4 for explanation of the process). Next the results from conducting the PIA is then presented, including the time spent in work hours. The two last sections of this chapter contains a summary of the findings and results from conducting the PIA. The findings relate to problems encountered while conducting the PIA, and the results relating to privacy risks. Throughout these two case studies, the risk analysis practitioners conducting the case studies are referred to as the "practitioners".

Conducting the privacy impact assessment did not possess any prior knowledge of privacy impact assessments, the time spent (section 8.2.4) on conducting this PIA is meant as guidance for first time practitioners. The practitioners possessed knowledge of ordinary risk assessment frameworks (such as ISOI/IEC 27005, NIST 800-30 and ISACA Risk IT) and stakeholder analysis. The practitioners also possessed some general knowledge about identity management systems, but no specific information about MinID.

8.1 Using the PIA framework

The Privacy Impact Assessment Handbook v2.0 is a framework for assessing impacts to privacy in systems that handle personal data. The framework presents a step by step method for detecting risks to privacy. It consists of an additional initial assessment and five main steps, these are presented in chapter 4. In this section each step of PIA process is discussed as the practitioners experienced them, and in addition some general comments on the framework are discussed.

8.1.1 Initial Assessment

One of the first things that were noticed during the work with PIA, is that the initial assessment was a big task and the information gathering process conducted to answer the screening questions was a time consuming job. The initial assessment produced a document that was used as a foundation for further PIA work. The initial assessment needs therefore to be taken seriously,

if the initial assessment is rushed through, then the whole PIA work will have a bad foundation and already be off to a bad start. The initial assessment process map can be seen in the previous chapter, figure 11.
The main task of the initial assessment is to be able to answer the screening questions in appendix A of the framework. The screening questions are divided into four different steps, illustrated in figure 27.

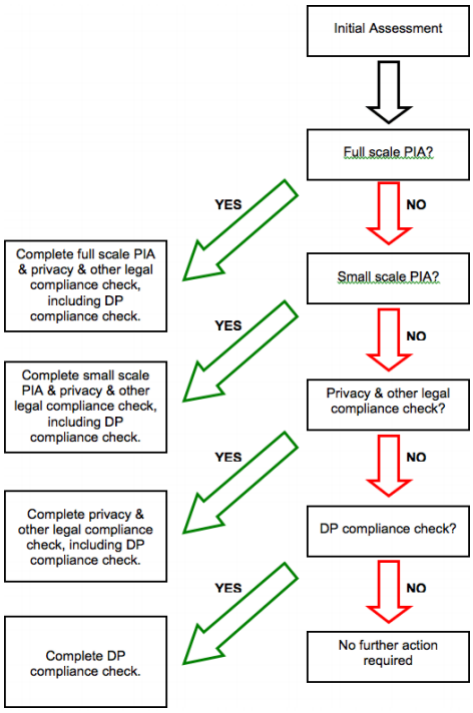


Figure 27: PIA screening process. *(Source: PIA [4])*

One of the first tasks PIA recommends doing is to create a project outline. The main goal of this task is to gather available relevant information and organize it. The outline should ideally consist of:

- Scope of the project.
- Features of the system.
- Aims and goals of the project.
- Project initiation documents.
- Existing laws and legislation relevant for the project.

This documentation is needed to answer the screening questions, and obtaining this information

is therefore critical to be able to answer them properly. This task was a straight forward information gathering task.
The next task PIA recommends, is to undertake a stakeholder analysis. The information related to this task is not extensive, it provides guidance for determining which stakeholders should be included, i.e. "organizations and individuals that are intended to benefit from it" and "the organization conducting the project, and perhaps also various sub-organizations within it". This guidance was helpful, and the amount of stakeholders was reduced to a little over a page. However, it does not provide any guidance on prioritizing stakeholders, classification or anything similar. Which is a point of criticism, as a reference to a stakeholder analysis methodology could have been provided. The practitioners have also found that the term "Stakeholder analysis" is highly subjective. The PIA framework states "undertake a stakeholder analysis", but the term analysis can mean very different things to different people. The term analysis in the PIA setting may only refer to the simple task of listing stakeholders, and prioritizing them to fit an A4 page. Subjectivity is a problem that pervades in the framework, which will be discussed later.
The last task of the initial assessment is to do an environmental scan, which consists of seeing what else is out there. No PIA reports were found for IdMS, but some related reports were found.

To be able to give satisfactory answers to the screening questions in the initial assessment, the assumption that the project was currently in the implementation/testing phase of the project was made. Since MinID is part of the digitization of Norway, the questions regarding change were answered with the transition from paper to digital public services as a basis. The complexity of the questions are generally high, and it takes time to answer them correctly. Out of the 71 hours spent on the initial assessment, 50 were used to answer the initial assessment questions. Some of the questions are formulated such that they need to be interpreted by the practitioner, i.e. question 6: "Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database", this raises questions about what "significantly changed handling" means? PIA does not provide any scale for measuring this, and it is left to the practitioner to determine what "significantly changed" means. The same goes for defining "a considerable amount of personal data", what is a considerable amount, and how is it measured? Adjectives is a problem when answering the screening questions, personal interpretations of each question can impact the total outcome of the screening questions and cause the wrong type of PIA to be conducted. Some other examples of terms that can be interpreted by the practitioner to fit his/hers purpose: "personal data silos", "substantial potential", "pseudonymously", "particular concern". Although taken out of their context, it is easy to see that these terms can be interpreted to fit the context of the practitioner's agenda.
The next issue with the screening process is that there is little guidance in the framework on how to conclude on the screening questions. It does not provide any measurable amount, such as "above four answered yes, then conduct a full-scale PIA". It encourages to view the answers to all the eleven questions as a whole, and conclude on this basis, which is the only real guidance the framework provides. This again leaves non-extreme conclusions to be very subjective, and both answers and conclusions can be purposely manipulated either way to fit the practitioners agenda (such as if the practitioner is an external consultant, the results can be manipulated such

that the organization will be in need of the practitioners services). The decision if an assessment is to be conducted and what kind is left entirely to the group or consultant conducting the initial assessment.

When the type of PIA was determined, the tasks that the assessment requires were outlined and put in a project plan. This project plan can be found as an appendix to the complete PIA report. However, in this project the Privacy Law and the Data Protection Act Compliance check are out of scope, as this projects scope is risks posed to privacy in identity management systems, and not risks posed by being non-compliant regarding privacy laws. The Handbook also suggests these two processes as separate process from the privacy impact assessment, and they are suggested as future work.

Initial Assessment Conclusions

The conclusions from the initial assessment is used to determine if a PIA should be conducted, and if yes, what kind. According to the Handbook, the eleven answered questions should be considered as a whole, and not individually, which means that the practitioner should conclude on the result as a whole. Which is the only guidance provided by the framework. Out of the 11 questions from appendix 1, seven were answered yes, two were answered no, and two questions was left inconclusive as the system documentation was not adequate to answer these two.
Together with the amount of yes from the question.the amount of people using MinID combined with the amount of personal data available through MinID, was also a strong argument for conducting a full-scale PIA. The PIA was conducted *system specific* for MinID, with weight on the authentication and authorization systems.
The initial assessment of the "Privacy Law Compliance"-check yielded a yes 3 out of 3 possible, and such a test should be part of the whole assessment. The conclusion was also that a "Data Protection Act"-compliance check is needed.

Ten identified privacy threats were detected as a part of the initial assessment (for the initial threats see the appendix of the PIA report, Initial Assessment). The process yielded an initial insight in to the systems privacy risks as it promised, but it was also a time consuming task, totalling 71 work hours.

8.1.2 Preliminary Phase

PIA [4] states that "The purpose of this phase is to ensure that a firm basis is established for the PIA to be conducted effectively and efficiently". The preliminary phase builds upon the work conducted in the initial assessment, another argument for doing the initial assessment thoroughly. This phase should produce a PIA project plan, and a project background document (both can be found in the appendix of the PIA report) which is a further development of the initial assessment document, some of the tasks in these two phases are also very similar. The preliminary phase

adds to the document with expanded project outline, context description, motivation, business rationale, justification of personal data handling, and further examination of the project stakeholders. The PIA framework explains the different tasks of this phase well, and it is easy to follow the tasks outlined in this phase. However, one of the main problems with this phase was that the tasks were scoped to fit the starting phase of the MinID project. The system that is being assessed is in one task referred to as a "proposal", which does not fit the context of the assessment performed in this thesis. But the framework also presents the solution for this problem: "If the project has already been through the requirements analysis and design phases, the project background paper can describe the flows of personal information at the appropriate level of detail. These may be placed in appendices containing diagrams that depict process descriptions and lists of items of personal data involved."
Since this project was based on open sources, some of the tasks in the preliminary phase were very limited and some were skipped entirely. The practitioners did i.e. not have preliminary discussions with representatives from the different stakeholder groups since there was no contact with these groups. But there is also reason to question the need for stakeholder consultation in this phase of the assessment, unless the practitioners have a good relationship with all the different stakeholders, arranging more than one meeting with each stakeholder may be unrealistic. And if the amount of meetings is limited to one, this meeting should take place in phase three, when the practitioners have a better overview of the privacy risks in the system and a better take on what to ask. Time limitations may also impact the amount of interviews and consultations that can be performed, it takes time both to prepare, conduct and process interviews.

As defined in the framework, the identified issues from the initial assessment was further examined and expanded in to threat scenarios for the risk analysis. The business case and the justification for handling personal data was emphasized in the document. Doing a thorough job in this phase as well, will reward the practitioners in the documentation phase. Our experience was that together with the initial assessment document, the project background paper was very useful for writing the final report.
The ten potential threats identified in the initial assessment was assessed as a part of this phase, and turned into concrete threat scenarios, which can be found in section 8.2.2, scenarios 16-25.

8.1.3 Preparation Phase

Suggested deliverables is a stakeholder analysis, a consultation strategy and plan, and the establishment of a PIA consultative group. The consultation strategy and PIA consultation group was not emphasized in the assessment of MinID, this was because of the practitioners positions as external consultants, and the fact that this assessment was based on open sources.
The most time consuming task in this phase was the stakeholder analysis. The threat identification tool described in chapter 6 was used to identify threats to privacy in addition to the threats that were discovered in the initial assessment.

8.1.4 Consultation and Analysis

The main goal of this phase is to identify the design issues and privacy problems with the MinID project through stakeholder consultations and risk analysis. As the framework recommends, much of the time in the consultation and analysis phase for the MinID assessment was spent on risk analysis. This was part of the process of identifying design issues and privacy problems with the project. These threats to privacy were documented and prepared for the final PIA report. The biggest problems that were encountered in this phase was regarding risk estimation. With more time available, a practitioner can consult with the stakeholder groups to get a better feel for likelihood and impact. The practitioners did not use the MEHARI tool for determining residual impact. Since this is a risk analysis for privacy, the view of the user was taken when considering impact to privacy. And many of the identified privacy risks have little or no impact on Difi. If a privacy risk really is going to hurt an organization it must be founded in some sort of offense.
Another problem with this phase was that the PIA framework does not suggest any risk analysis tools that are recommended for detecting risks to privacy. Such a recommendation or guideline for choosing a tool would have been a nice addition to the standard.

8.1.5 Documentation Phase

The purpose of this phase is to show that the PIA process was performed appropriately, provide basis for reviews and audits, and documentation in general. This part of the framework describes what the purpose of the report is, and what it should contain. This phase was used to document all the work and produce a PIA report (see appendix A). The PIA report was written according to the framework, and with the expectation that it might be published or widely distributed. With specific purpose of being a source of input and background information for people conducting PIAs in the future. The framework is clear on what the PIA report should contain, and what information sources should be used for the task.

8.2 Privacy Impact Assessment Results

In this section the results from conducting the PIA is presented. The privacy risks identified using the stakeholder analysis and the initial assessment is first presented, then the relevant threat scenarios originating from these risks are listed. And the section is ended with the results from the adapted version of the MEHARI risk analysis.

8.2.1 Stakeholder Analysis Results

The stakeholder analysis was conducted using the stakeholders presented in chapter 7 and their attributes. The first 15 scenarios in the table on the next page is the scenarios identified from the stakeholder analysis, where privacy is negatively affected. Scenarios sixteen to twenty five are

the threat scenarios from the initial assessment/preliminary phase adapted to the stakeholder analysis. Although they were already privacy threat scenarios, we chose to analyze them using the stakeholder analysis to see if they were transferable to the method, and to see if some of the scenarios were redundant (same privacy threat scenario discovered by both methods).
Each stakeholder has a set of capabilities that he/she can choose to act upon. Some of the capabilities are similar actions, and have therefore been grouped together for the sake of making this task smaller. This list is non-exhaustive and there has been made an effort by the authors to only include the scenarios that can relate to privacy issues (capabilities that affect privacy in a negative way).

Scenario nr	ACTOR	CAPABILITY	ASSET(s) AFFECTED (Positive or negative)	EFFECT *(for stakeholder)*	AFFECTED STAKEHOLDERS (Positive or negative)
1	1.1 Difi Mangement	- Retain funding from security measures - Increase funding on other measures	- System Security (-) - Security Policies (-) - Internal funds (+) - Revenue (+) - Subscriber Privacy (-)	- Free up funding for other projects within Difi or MinID, which can increase revenue and improve usability for the *Users*.	- Internal threat agents (+) - External threats (+) - Users (-)
2	1.2 Difi Deparments	Customer service: - Access MinID database (Read) - Write to database information (Write)	- Subscriber privacy (-) - Goodwill (+) - Revenue (+)	- *User* increases in satisfaction, a small reduction in privacy, because of data accessed - Increase in Goodwill, which may implicate more revenue gains Difi management - Gains External attacker, opens potential attack path.	- User (-) - Difi management (+) - External Attacker (+) - Competition (-)
3	1.2 Difi Deparments	- Access to high level logs (Read\write) - Merge high level logs	- System security (+) - Subscriber privacy (-) - MinID DB information (+)	- Increase in system integrity and security, as merging of logs can help detect anomalies in the system. - Privacy issues for the *Users* regarding logs. - *Internal threat agents* gets access to more sensitive information, when database increase in value. - Opens possibility for cross referencing sites the user accessed at which times.	- User (-) - Internal threat agents (+)
4	1.3 Malicious Insider and Non-compliant employees	Read/Copy Datamining Masquerade Espionage Selling information	- MinID database (-) - User subscription list (-) - MinID User logs (-) - System Documentation (-) - System Security Information (-) - Subscriber privacy (-) - Cash (+) - Anonymity (-) - Knowledge / Trade secrets (-)	- Obtain information about *User(s)* and *Internal actors (Difi)* - Lose Anonymity - Gain cash by selling information	- User (-) - Interal actors (-) - Competitors (+) - Attackers (+)
5	1.3 Malicious Insider and Non-compliant employees	Corrupt or Delete	- MinID database (-) - System Documentation (-) - MinID User logs (-) - User subscription list (-) - Anonymity (-) - Subscriber privacy (-)	- Corruption/removal of data from *Internal actors (Difi)* causing loss of availablity - *Internal actors* loose revenue	- User (-) - Internal actors (-) - Competition (+)
6	1.3 Malicious Insider and Non-compliant employees	Attack	- MinID database (-) - User subscription list (-) - MinID User logs (-) - System Documentation (-) - System Security Information (-) - Anonymity (-) - Subscriber privacy (-)	- Disrupt availability for *User(s)*, *Internal actors (Difi)*, *Service Providers*. - *Internal actors* loose revenue - Inflicts *Government* looses goodwill from the people. - Attacker may publish privacy related information	- User (-) - Internal actors (-) - Competition (+) - Government (-)

Scenario nr	ACTOR	CAPABILITY	ASSET(s) AFFECTED (Positive or negative)	EFFECT *(for stakeholder)*	AFFECTED STAKEHOLDERS (Positive or negative)
7	2.1 Regulatory Services	- Decrease funding - Penalize Difi - Shutdown project	- Funds (+) - Goodwill (-) - Reputation (-) - Subscriber privacy (-)	- Funds increase due to decrease in Difi funding, penalties or shutdown. - Goodwill is reduced due to less funding. - Loss of Reputation can occur given that the government has a direct stake in the MinID solution. - Funding for Privacy security for *Internal actors* is decreased	- Difi Management (-) - Difi ICT (-) - Competition (+) - Users (-)
8	3.1 Users	- Register	- MinID database (+) - Privacy (-) - Availability (+)	- User is registered in the *Difi* database for users - Registers personal information with a third party.	- Internal actors (+) - Competition (-) - ID-Portal (+) - Governmetn (+)
9	3.1 Users	- Log in/out (authenticate) - Use services in ID-Portal - Order PIN codes - Change personal information	- MinID database (+) - Privacy (-)	- The logs in MinID database increase in information and gain value. - Increase in logs puts privacy of the user is in jeopardy. - Number of log ins gains Internal actors	- Internal actors (+) - Government (+)
10	4.1 Competitors	- Influence users - Innovate/implement new functionalities	- Funds (-) - Revenue (+) - Subscriber privacy (-)	- More investments in influencing users and improving software attracts more users, but drains funds. - User shares personal data with another actor	- Interal actors (-) - Users (0) - Government (-)
11	4.1 Competitors	- Log userinfo - merge logs	- Subscriber privacy (-) - Database information (+) - User logs (+) - Security (+)	- Privacy issues for the *Users* regarding logs. - Opens possibility for cross referencing sites the user accessed at which times.	- User (-)
12	4.2 ID-portal	- Provide personal data for eID providers	- Personal data (-) - Subscriber privacy (-)	- Personal data is shared with MinID (or other eID provider). - Privacy is weakened for the *Users* through sharing of personal data.	- Users (-) - Internal actors (+)
13	4.2 ID-portal	- Genereate PIN-codes - Send PIN-letter - Send PIN- SMS	- Pin codes (+) - Subscriber privacy (-)	- Stakeholder uses third party to distribute PIN codes to *Users*. - Privacy is weakened since third party obtains knowledge about the *Users* registering with MinID	- Users (-)
14	5.1 Attackers	- Automated attacks - Targeted attacks	- Anonymity (-) - Personal data (+) - Sensitive personal data (+) - System documentation (+) - System security settings (+) - Cash(+) - Subscriber privacy (-)	- Attacker looses anonymity if the attack is detected. *If attack is successful:* - Attacker gains one or more of the assets he wants.	- Internal actors (-) - Users (-) - Government (-) - Competition (+)
15	5.1 Attackers	- Buy personal data - Hack accounts - Register new user with unregistered birthnumbers (in Difi DB)	- Anonymity (-) - Cash (-) - Personal data (+) - Sensitive personal data (+) - Birth numbers (+) - Subscriber privacy (-)	- Attacker runs risk of loosing anonymity, when he interacts directly with traders, or interacts directly with the system. - Attacker gains personal data and birth numbers and use this for further attacks or data mining.	- Internal actors (-) - Users (-) - Government (-) - Competition (+)
16		*Covered in scenario 4*			
17	5.1 Attacker	ID-theft based on birthnumber	- Subscriber privacy (-) - Cash (+)	- This attack can be effective on unregistered users, if the attacker possess birthnr and mailbox address.	- Users (-)

Scenario nr	ACTOR	CAPABILITY	ASSET(s) AFFECTED (Positive or negative)	EFFECT *(for stakeholder)*	AFFECTED STAKEHOLDERS (Positive or negative)
18	1.1 Difi Mana. 1.2 Difi ICT	Function creep on Birth number	- Subscriber Privacy (-) - Usability (+) - Funds (+)	- The purpose of the identifier increases, and the identier contains personal information about the user.	- Users (-)
19	1.1 Difi Mana. 1.2 Difi ICT 4.2 ID-portal	Loose sensitive personal data during digitalizing of services (accidental or intentional)	- Sensitive Personal data(-) - Subscriber privacy (-) - Reputation (-) - Revenue (-)	- Leak affecting privacy of users - Likely that relationship with regulatory services is weakened - Competition gains revenue - Ext threats gains opportunity to buy sensitive data.	- Users (-) - Regulatory services (-) - Competitors (+)
	1.3 Internal threat agents		- Subscriber privacy (-) - Cash (+)		- Users (-) - Ext Threat agents (+)
20		*Covered by scenarios 12 & 13*			
21		*Covered by scenarios 4 & 15*			
22		*Covered by scenario 15*			
23	1.1 Difi Mana. 1.2 Difi ICT	Add security measure without regarding privacy implications.	System security (+) - Subscriber privacy (-)	- Increase in system integrity and security, through some added measure - Privacy issues for the *Users* regarding new measure - *Internal threat agents* gets access to more sensitive information.	- Users (-) - Internal threat agents (+)
24 & 25 (*Similar scenarios)*	1.1 Difi Mana. 1.2 Difi ICT	Disregard laws, legislations, regulations or policy when handling personal information.	- System Security (-) - Security Policies (-) - Revenue (-) - Subscriber Privacy (-) - Goodwill (-) - Reputation (-)	- Decrease in system security increases chances for security incident. - Decrease in privacy for *Users*. - Increase in chances of auditing being needed, and negative consequences of auditing increses - Competitiors gains revenue	- Internal threat agents (+) - Regulatory Servicest (-) - Users (-) - External threats (+) - Competitors (+)

8.2.2 Threat scenarios from Stakeholder Analysis and Initial Assessment

These privacy threat scenarios were identified using the results from the stakeholder analysis. One privacy threat scenario has been created for each analyzed capability.

1. Difi Management chooses to retain funding for security measures, and increase funding for other functionalities.
2. Difi Departments choose to access (read/write) MinID subscriber database as a part of quality improvement of services provided by i.e. customer service.
3. Difi Departments chooses to access high level logs (read/write), and merge them for security purposes (i.e. merge log ins to detect anomalies, such as if a frequent user who normally logs in from Norway suddenly logs in from China).
4. The Malicious Insider reads and copies system information (including MinID database) for malicious purposes, such as espionage, datamining or selling of personal data.

5. The Malicious Insider chooses to access the MiniD database to corrupt or delete data in the MinID IdMS, i.e. to hide or corrupt data about a citizen.
6. The Malicious Insider chooses to launch a full scale attack on the system, i.e. to execute revenge on a perceived injustice.
7. Regulatory services chooses to decrease funding (or shut it down) for the MinID project, resulting in less money for security purposes.
8. User chooses to register with the MinID service, which shares the users personal data with a third party.
9. User chooses to make use of the services provided by MinID at a daily basis, causing the value of the MinID database to grow with more personal information about the user.
10. Competitors of MinID chooses to spend money on a developing new functionality to attract users of MinID over to their own system, causing the users to share information with another third party.
11. Competitors log user information and merge these logs for security purposes, causing these logs to grow in size and increase in value.
12. The service providers in the ID-portal chooses to share personal data with the eID providers to help increase quality of service.
13. The service providers in the ID-portal uses a third party to send PIN-codes to the users for two factor authentication, allowing third parties to gather information about the users of MinID.
14. Attackers choose to attack the MinID system, either through automated or targeted attacks, to steal information. If successful the attacker can obtain sensitive information that he/she can sell for cash.
15. Attackers choose to buy personal data (i.e. from malicious insider) to exploit for further use, i.e. to reveal the location of hidden persons or blackmail.
16. (PIA) Since Difi maintains a database that stores user personal password, PIN, telephone number, social security number and behavior logs. The Malicious insider can choose to use the information kept in the logs for *surveillance, locating and tracking* individuals.
17. (PIA) MinID re-uses a multi-purpose identifier (social security number) as a part of the authentication process. The social security number can scarcely be regarded a secret, and an attacker may choose to misuse (i.e. ID-theft) the social security number of a citizen (i.e. registering MinID and steal the snail mail with PIN codes).
18. (PIA) MinID re-uses a multi-purpose identifier (social security number) as a part of the authentication process. Difi may choose to expand the use of the social security number for quality of service or ease of access. So called "function creep".
19. (PIA) Sensitive personal data getting lost or leaked to a third party during the digitalizing of the public services the handling of information changed from mainly paper-based to digital handling.

20. (PIA) Personal data getting lost or leaked to a third party during the digitalizing of the public services, when the handling of information changes from mainly paper-based to digital handling. The MinID database also contains telephone numbers of the users. This information can be sensitive for a small percentage of the population who wants to keep their numbers confidential to avoid being found.
21. (PIA) The project handles a considerable amount of log ins and data about an individual. This data being sold to consumer marketing based on intensive profiles. It also opens for the possibility of data gathering and mining, as well as data matching. Information can also be used for surveillance, locating and tracking.
22. (PIA) The project does handle personal information concerning a large amount of individuals. This makes the system attractive to organizations and individuals trying to locate people or build marketing profiles.
23. (PIA) Increase in security measures impact a large amount of the population. The added security measure does not give privacy enough concern, and intrudes the privacy of users.
24. (PIA) The system offers functionalities that are subject to a number of laws regarding privacy. Relevant laws are not taken into account.
25. (PIA) Difi is according to Norwegian law defined as a data handler, and handles personal data and facilitates access to sensitive data about natural persons. They disregard laws and regulations, or do not realize that they are defined as a data handler.

8.2.3 MEHARI Privacy Risk Analysis Results

In this section the results of the MEHARI risk analysis is presented, together with a discussion of the privacy issues and implications of the project.

Risk Likelihood

Explanation to likelihood calculations together with attribute evaluation can be found in section 6.2, and examples of probability calculation can be seen in figure 22. The values used for calculations can be found in the appendix D, and the detailed sheets for calculation can be found in the PIA report (appendix A). Figure 28 illustrates the adapted residual likelihood calculations from MEHARI. Residual likelihood has been calculated for each identified privacy threat scenario.

Residual Likelihood

Scenario nr	Actor	Knowledge level	Assets rewarded	Assets Risked	Relationship rewarded	Relationships risked	Intrisic likelihood <1>0	Control effiency <1>0	Residual Likelihood
1	Diffi Management	0,6	0,3	0,3	-0,2	0,05	0,7	0,35	0,35
2	Diffi Departments	0,6	0,25	0,15	-0,1	0,05	0,5	0,2	0,3
3	Diffi Departments	0,6	0,2	0,15	-0,1	0,05	0,8	0,2	0,6
4	Internal threat agents	0,6	0,15	0,3	0,15	-0,3	0,9	0	0,9
5	Internal threat agents	0,6	0,15	0,3	0,05	-0,3	0,8	0	0,8
6	Internal threat agents	0,6	0,15	0,45	0,05	-0,3	0,8	0,15	0,65
7	Regulatory Services	0,4	0,15	0,35	0,05	0,3	0,6	0,65	0,01
8	Users	0,4	0,2	0,15	0,15	0,05	0,75	0,2	0,55
9	Users	0,4	0,2	0,15	0,1	0	0,7	0,15	0,55
10	Competitors	0,6	0,25	0,25	0	-0,05	0,85	0,2	0,65
11	Competitors	0,6	0,35	0,1	0	0,05	0,95	0,15	0,8
12	ID-portal	0,2	0,15	0,25	0	0,05	0,35	0,3	0,05
13	ID-portal	0,2	0,2	0,15	0,2	0,05	0,55	0,2	0,35
14	External Attackers	0,4	0,3	0,5	0,05	-0,4	0,75	0,1	0,65
15	External Attackers	0,4	0,3	0,3	0,15	-0,4	0,95	0	0,95
16	*See scenario 4*								
17	External Attackers	0,4	0,15	0	0	-0,1	0,55	0	0,55
18	Diffi manag + ICT	0,6	0,25	0,15	0	0,1	0,85	0,25	0,6
19a	Diffi manag + ICT, ID-portal	0,4	0	0,6	-0,1	0,15	0,3	0,75	0,01
19b	Internal threat agents	0,6	0,15	0,05	0,1	-0,1	0,85	0	0,85
20	*See scenario 12&13*								
21	*See scenario 4 &15*								
22	*See scenario 15*								
23	Diffi manag + ICT	0,6	0,15	0,15	-0,1	0,05	0,55	0,2	0,35
24 & 25	Diffi manag + ICT	0,6	0	0,8	-0,3	0,15	0,3	0,95	0,01

Figure 28: Risk Likelihood.

Risk Estimation

The classification of each risk scenario is seen in figure 29. Each threat scenarios is categorized according to the taxonomy of privacy risks presented in this thesis (see section 5), and the worst case impact determined in the questionnaire (see section 17). Risks displayed as recommended

Scenario	Likelihood of occurance	Privacy Risks (Classification)	Privacy Impact	Risk Seriousness
1	Medium	Insecurity	Very High	High
2	Low	Increased Accessibility	High	Medium
3	High	Surveillance, Aggregation	Very High	Very High
4	Very High	Breach of Confidentiality, Disclosure	Very High	Very High
5	Very High	Distortion	Very High	Very High
6	High	Insecurity, Breach of Confidentiality	Very High	Very High
7	Low	Insecurity, Legal Consideration	Very High	Medium
8	High	Denial of Anonymity, Function Creep	Very High	Very High
9	High	Aggregation, Surveillance	High	High
10	High	Surveillance, Identification	Very High	Very High
11	Very High	Surveillance, Aggregation	Very High	Very High
12	Low	Denial of Anonymity, Secondary Use	Very High	Medium
13	Medium	Denial of Anonymity, Surveillance	Very High	High
14	High	Breach of Confidentiality	Very High	Very High
15	Very High	Breach of Confidentiality, Disclosure	Very High	Very High
17	High	Breach of Confidentiality, Blackmail	Very High	Very High
18	High	Function Creep, Secondary Use	Very High	Very High
19a	Low	Insecurity, Disclosure	Very High	Medium
19b	Very High	Insecurity, Disclosure	Very High	Very High
23	Medium	Decisional Interference, Surveillance	High	Medium
24 & 25	Low	Legal Consideration	Very High	Medium

**Scenarios 16, 20, 21 and 22 are covered by scenarios 4, 12, 13 and15.*
***Scenario 19 is divided because of equal scenario with different actors.*
**** Scenario 24 and 25 is combined because of their resemblance.*

Figure 29: Privacy threat scenarios analyzed and categorized within privacy risk classes.

by MEHARI can be seen in figure 30. Due to the results from the questionnaire, each risk is present at the upper half of the matrix. With a more specific method for assessing impact, it is likely that some of these threat scenarios would be place lower in the matrix.

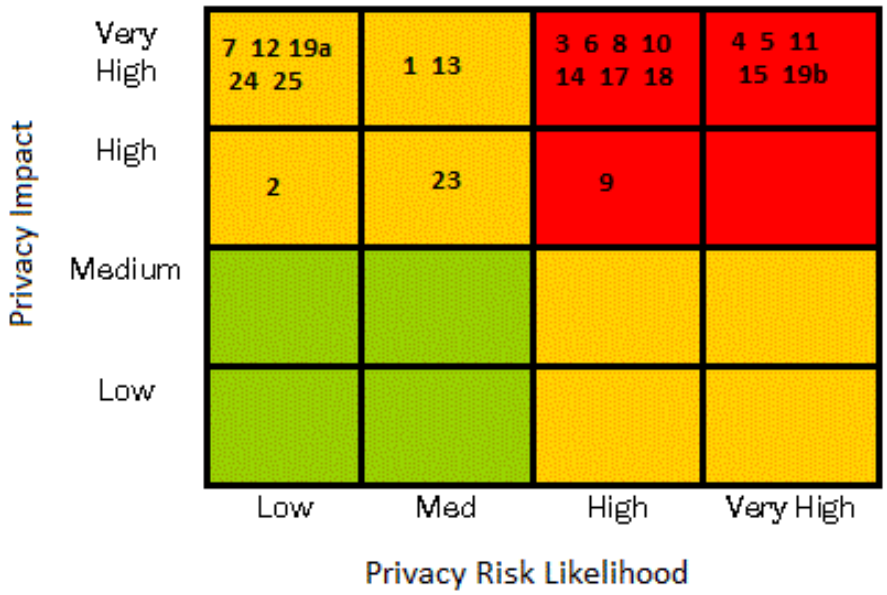


Figure 30: Privacy Risk Seriousness Matrix

8.2.4 Use of time

The total time spent on each PIA task and total time use is illustrated in figure 31. The total amount of time spent on conducting the PIA was 187 hours, where the majority of time was spent on the initial assessment and preliminary phase. This result will be discussed in chapter 10.

Privacy Impact Assessment, Time use	
Task	**Total hours**
Initial Assessment	71
Preliminary Phase	14
Preparation Phase (SH analysis)	51
Consultation and Analysis phase	30
Documentation Phase	21
Review and Audit Phase	0
	187

Figure 31: PIA total time use

8.3 Summary of findings using the PIA framework

- The initial assessment is a time consuming task, and should, together with the preliminary phase, be completed thoroughly since the rest of the PIA work will be founded on this work.
- Interpretations of terms is a prevailing problem throughout the initial assessment. The use of adjectives in the initial assessment allows for interpretations of questions.
- The guidance for concluding on initial assessment is very limited, and close to non existent.
- PIA does not provide any guidance on prioritizing stakeholders, classification or anything similar.
- The term "Stakeholder analysis" is highly subjective. The PIA framework states "undertake a stakeholder analysis", but the term "stakeholder analysis" can mean very different things to different people. The term analysis in the PIA setting may only refer to the simple task of listing stakeholders, and prioritizing them to fit an A4 page, or doing an advanced analysis, i.e. the one performed in this thesis.
- The PIA framework does not suggest any risk analysis tools that are recommended for detecting risks to privacy.

8.4 Summary of Results using the PIA framework

- Total time use was 187 hours.
- Initial assessment: the conclusion was that a full scale system specific PIA was to be conducted.
- Initial assessment: 10 potential privacy threat scenarios were discovered.
- Preliminary phase: PIA project plan, project background document, refined privacy threat scenarios.
- Preparation phase: Stakeholder analysis produced 15 privacy threat scenarios, which together with the risks from the initial assessment produced 21 individual privacy threat scenarios.
- Consult and Analysis phase: 37 risks to privacy were found when analyzing the 21 privacy threat scenarios.
- Documentation phase: Produced a complete PIA report with discussions of MinID solutions and proposals for mitigation measures and risk management strategy. Appendix A.
- Of the 19 privacy risk classes, PIA identified risks within 14 of them.

9 Case study 2 - Risk IT

The second case study in this thesis was conducted using the The Risk IT Framework [5] and The Risk IT Practitioner Guide [15], both published by ISACA in 2009. This case study was performed on the scenario presented in chapter 7.
This chapter contains comments on using the Risk IT framework for the purpose of detecting privacy risks, findings, and time spent on this approach. The two last sections of this chapter contains a summary of the findings and results from conducting the Risk IT approach.
The Risk IT report found in appendix B is a simplified report which consists of Risk Universe, Risk Scenarion Identification and Risk Analysis. The purpose of the Risk IT report was to form the basis for comparison with the findings of PIA.

The disregarded information security risks detected in the case study may also lead to privacy risks in the future, but for the sake of thesis length and complexity, risk analysis has only been conducted on risks that visibly affects the user.

9.1 Using the Risk IT

It took less time to begin the risk analysis process using Risk IT as this approach was familiar to the practitioners. As defined in section 1.6, the scope of this analysis was to be risk identification and risk analysis. To be able to conduct these two activities, a scenario description is needed, which is defined as a "Risk Universe" in the Risk IT framework. This section consists of an evaluation of these three activities.

9.1.1 Defining the Risk Universe

The task of defining a risk universe consists of defining the scope and scenario description for the risk analysis process. The task of scoping the risk analysis process is left entirely up to the practitioners in Risk IT, the framework provides guidelines for what is recommended to have present in the risk universe: "a risk universe describes the overall (risk) environment (i.e. defines the boundaries of risk management activities) and provides a structure for managing IT risk." The risk universe should ideally contain business objectives, business processes and their dependencies, and the IT applications and IT infrastructure which support the business objectives. As with the scenario description (chapter 7) the risk universe of this analysis did not go beyond the boundaries of the MinID system.

Although risk appetite and tolerance are important factors in Risk IT, they are not important in this case study, this is because the focus is on detection and evaluation of risks to privacy. This case study does not suggest a risk management strategy based on these two factors, in this project they were only used to adjust the risk level matrix.
Risk IT states that the full value chain of the enterprise should be considered, the value chain constructed for this analysis can be seen in figure 32. This figure illustrates what is believed to be the most important value chain in Difi. A short explanation of the value chain is as follows, quality of service (QoS) affects the number of users choosing MinID as their eID provider. The amount of users affects how much funding the Government is willing to delegate to Difi and the MinID project, which again regulates the amount of funding available for improvement of QoS.

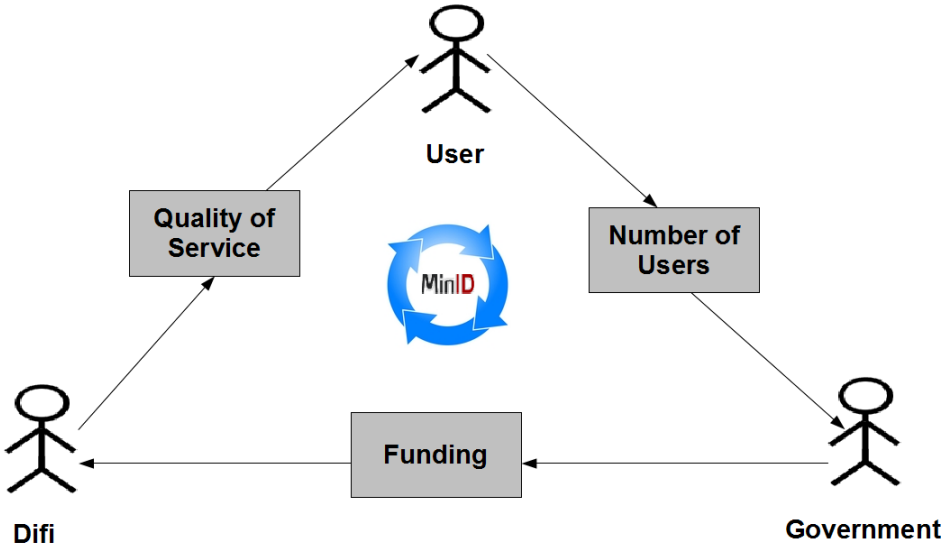


Figure 32: Main value chain for MinID

9.1.2 Risk Scenario Identification

For risk scenario identification the top down scenario identification approach was used. The approach chosen for this case study differs from what is recommended in the Risk IT framework. Risk IT suggests to identify the business objectives and identify the scenarios with most impact on achievement of the objective. Since the risk identification process in PIA already had been conducted, the practitioners felt that the brainstorming process would be heavily influenced by the already known privacy risks in the system, and a more objective approach was needed. Data flow diagrams/threat modeling were chosen for threat identification because of the practitioners' familiarity with this approach, and it provides an objective view of the system processes. The DFD models are based on a "best effort" using the system documentation available. The processes that are of interest in the system are those that handle personal data. The DFD model which depicted in figure 33 is a basics representation of the system. It shows all the terminators (actors) who

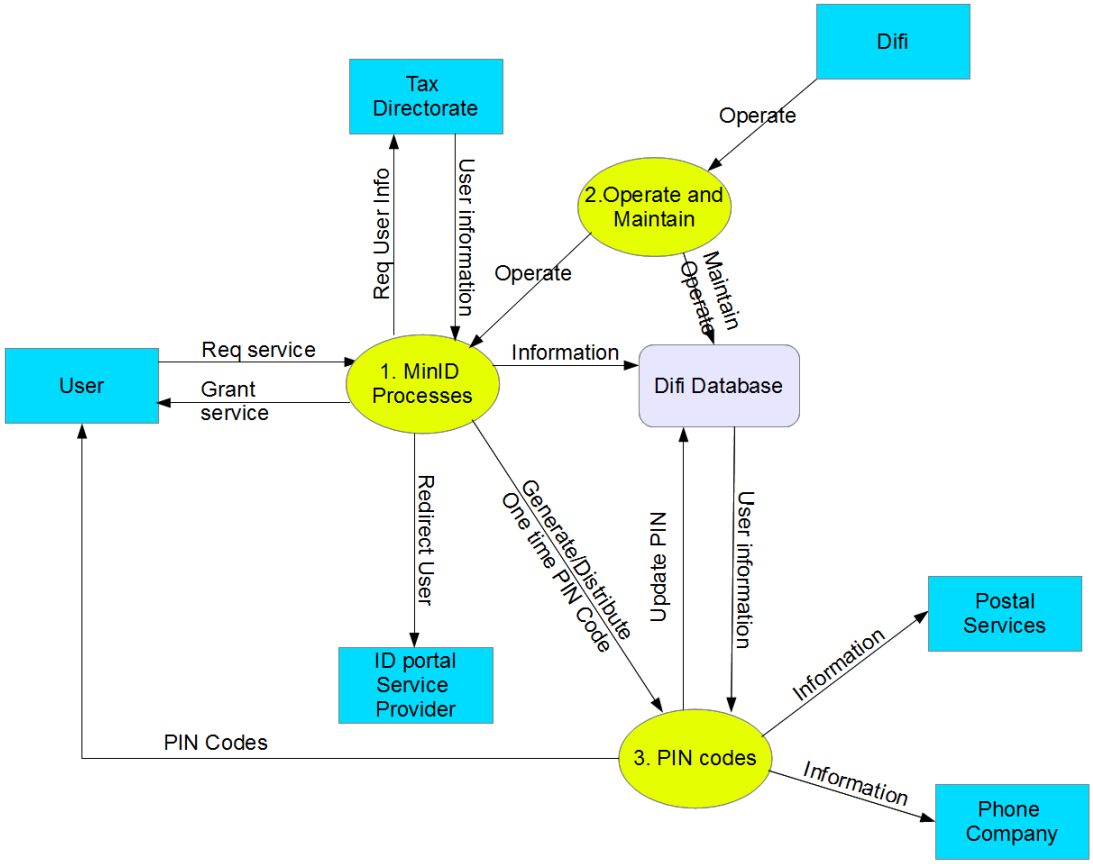


Figure 33: DFD top level process chart.

are part of the system, and how they are involved in MinID. The top level process chart has three processes, the workings of these processes will be addressed going one level deeper in the DFD process analysis.
The two models, figure 34 and figure 35, address the processes from figure 33, and show the inner workings of the models. For each of these processes, possible information security breaches of the data flows going in or out from the process will be analyzed to detect risk scenarios. A short explanation of the processes in the DFD are as follows:

1. Register new user: Unregistered user uses this process to register in the system. The process requires the user's SSN and personal data.
2. Fetch citizen data: This process uses the SSN to retrieve personal data registered about the user from the Tax Directorate Peoples register, and send it to the Difi Database.
3. Generate PIN Codes: Generates PIN codes for PIN letters users, and adds these to the letter from the Tax Directorate. It also adds the PINs to the Difi Database.

4. Send PIN letter: Is a process located in a third party, the postal services, which distributes PIN letters.
5. Authentication (Log in): Uses the SSN, password and PIN code for authentication. PINs are either from one-time PIN function or PIN letter.
6. Maintain Profile: Allows the user to maintain his personal data in the Difi Database. The personal data that can be updated is found in the yellow bubble in figure 25.
7. Generate One time PIN: This function generates a one time PIN for the user. This PIN is sent to the authentication process and the Mobile telephony service provider.
8. Check for Abuse/Error: This is the error and abuse checking process, it checks for inconsistencies in the Difi Database and Difi High Level Database.
9. Send PIN code: Sends the one time PIN code to the registered cellphone number of the user.
10. Order New PIN-letter: Allows the user to order a new PIN letter.
11. Block PIN letter: This process blocks the PIN codes in the PIN letter. The user must now authenticate using one time PIN codes to the cellphone.
12. Account Service: is a process that can be contacted by the user for help with the account, either through cellphone or e-mail (possibly other means). This process is operated by humans that have access to the Difi databases.
13. Reset Password: This process helps the user reset a forgotten password.

The processes depicted in the data flow diagrams (figure 34 and figure 35) were created using information from the user manuals for MinID [63] and other sources found in the scenario description. The data flow diagrams may not be entirely correct since they are based on open sources. One possibility in DFDs is to explore each process's inner workings, but to reduce complexity the system representation were limited to two levels as a representation of the system.

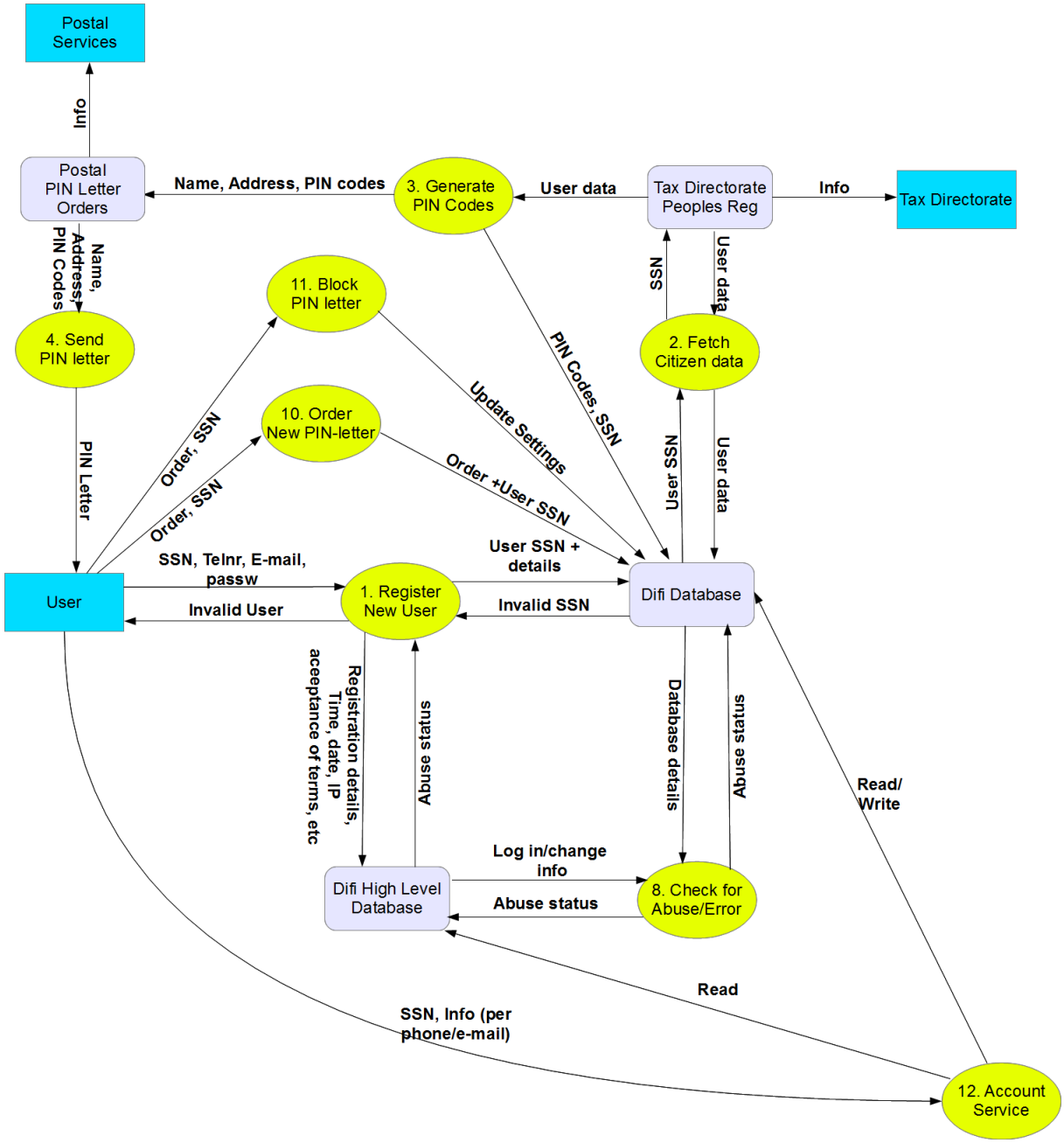


Figure 34: DFD process analysis 1

Time was not spent on examining attack vectors for scenarios that contained no obvious threat to privacy, and to limit scope of the DFD threat identification, technical vulnerabilities were not examined. More privacy risks may have been detected by combining the different risk scenarios, adding more capacity to the attacker.

The two DFD diagrams can be seen in figures 34 and 35, a more detailed analysis of each process can be found in the Risk IT report, appendix B. Designing two models level 1 models instead of one, gave a better overview of the system, and avoided process flows being crossed in the charts, as well as for presentation purposes.

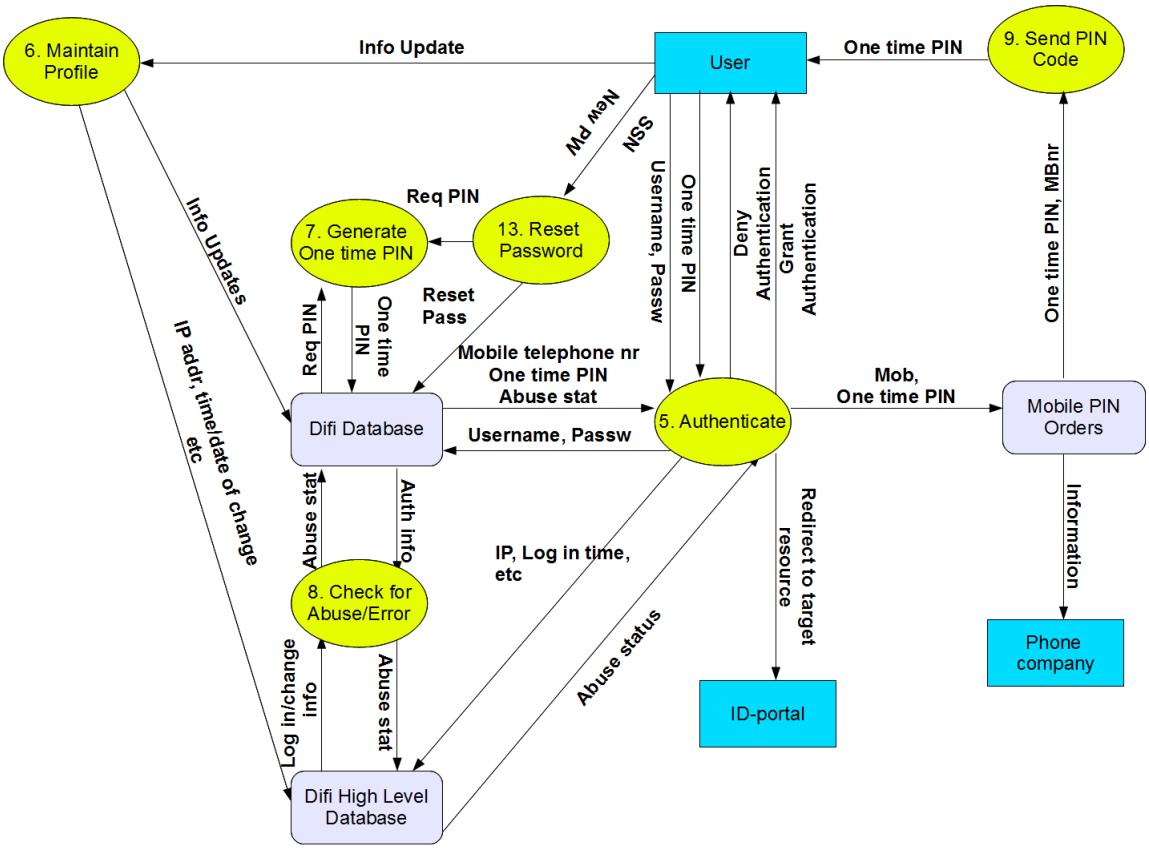


Figure 35: DFD process analysis 2

The risks discovered using DFD were of a more technical nature, as this approach considers system processes and information security threats to data flows. After the models were finalized, each data flow going in or out of each process was analysed assessing breaches to confidentiality, integrity and availability. This process yielded a dataset containing around 140 information security risks. To reduce the number of risks, the criteria of privacy related risk was added. This critera was simply answered "yes" or "no" after an assessment of the identified risk.

9.1.3 Risk Analysis

The Risk IT framework used in this thesis has been adapted to analyze risks to privacy. Which opens the question about who owns the discovered risks? A "Risk owner" is defined by ISACA as [15]: "Person or entity with the accountability and authority for managing the risk and any associated risk treatments." Per this definition, there is no straight forward answer to whom is the risk owner of this analysis. As privacy risks can be owned by both the user and the service provider. I.e. if an attacker breaches the computer of an user, and manages to hijack a session, it is likely that the user is the owner of the risk. This is because the breach happened at the users property through exploitation of some present weakness, and it is likely that the incident could have been avoided had the user followed basic security guidelines. In the explained scenario, the user is the risk owner because he has both accountability for the risk, and responsibility for managing the risk. Now in a scenario where a breach occurs within MinID, by i.e. illegal access to a database containing personal data, the user can not be held accountable (unless the user has signed a disclaimer depriving the service provider of any accountability). However, if one step is taken back in time, the risk owner is the user. Although there exists some "social pressure" to make users utilize electronic solutions to access public services, they do not have to. Since the choice of using MinID is the user's, and all of the risk scenarios in this analysis ultimately impacts the user, the risk owner in this analysis is the user.

The risk analysis conducted in the Risk IT report, was founded on subjective values for likelihood of occurance determined by the practitioners. Each risk was estimated using the frequencies:

1. The risk is likely to occur once per 48 months or less.
2. The risk is likely to occur once per 36 months.
3. The risk is likely to occur once per 24 months.
4. The risk is likely to occur once per 12 months.
5. The risk is likely to occur once per 6 months.
6. The risk is likely to occur once per 3 months.
7. The risk is likely to occur 1 time each month.
8. The risk is likely to occur 1 time every other week.
9. The risk is likely to occur 1 time every week.
10. The risk is likely to occur multiple times each week.

9.2 Risk IT Results

In this section the results from conducting the Risk IT assessment is presented. The privacy risks identified using threat modeling is first presented, then the relevant threat scenarios originating from the risk identification process are listed. And the section is ended with the results from the Risk IT risk analysis.

9.2.1 Identified threat scenarios

All of the privacy related risks were assessed by the practitioner, to weed out the risks with no vulnerability and the risks that were very unlikely to manifest. Example of an analysis of the DFD models is seen in figure 36, the complete analysis can be found in the Risk IT report (appendix B).

Process nr + Name	**Data flow name**	**Availability** (Column two is used to indicate privacy threat)		**Confidentiality** (Column two is used to indicate privacy threat)		**Integrity** (Column two is used to indicate privacy threat)	
1. Register New User	SSN, Telnr, E-mail, passw	- Cutting this can lead to DoS Ext attacker: can be done with a DdoS vs the user. This presents no imminate privacy risk, as this DoS must be prolonged to a serious amount of time to qualify as «Exclusion».	No	- Breaching the C(onfidentiality) of dataflow can be used to reveal User info. Can be done by breaking encryption and eavesdropping, or malware.	Yes	- Attack on this flow can allow the attacker to hijack the session. Can be accomplished on unregistered users, and through technical attacks.	Yes
	Invalid User	- Cutting this flow would only deny the user his invalid log in information. Ext attacker: DdoS vs server.	No	- Breaching the C of this dataflow can yield information about the registration status of the user. Eavesdrop or Malware	Yes	- Being able to compromise this flow will make the attacker able to DoS the User. Compromising the server, or hijacking server.	No

Figure 36: DFD privacy risk identification

The Risk IT framework states that the number of risk scenarios should be reduced to a managable set, the number of scenarios derived from the threat modeling process was 25:

1. External attacker breaches the confidentiality of the user's computer when registering for MinID, revealing SSN, chosen password, e-mail and mobile telephone number, identity theft using i.e. malware (or other computer attacks).
2. External attacker hijacks unregistered users' accounts through knowledge of victims SSN and postal address.
3. External attacker uses malware to compromise the user's computer and hijack the session when the user authenticates.
4. User is kept from his data due to a prolonged DoS attack on the service, leading to exclusion from his personal data.
5. Internal attacker reveals the data flows going in to the Difi database and the flow going out of the database, he can now data mine the data flows of SSN, passwords and one time PIN.
6. Internal attacker data mines first time registration detail flow going to high level database,

and uses this information for aggregation.

7. Internal or external attacker compromises the process that collects data from the tax directorate, and manipulates input to data mine the tax register and/or corrupt the Difi database.
8. Internal or external attacker eavesdrops stream from the external tax register database to Difi database and data mines this stream.
9. External attacker reveals the content of the PIN letter and is able to reset the user's account password, hijacking the account.
10. External threats data gather the one-time PIN and telephone numbers when they are sent through mobile telephone services.
11. Mobile services collapse, creating a DoS for the users.
12. Hacker attacks compromise the Difi databases, leaking information about the users to the Internet.
13. Internal or external attacker compromises user sessions with ID-portal and gathers sensitive personal data.
14. Internal attacker eavesdrops information going to the high level database.
15. User is identified in the MinID system where he only needs to be authenticated and authorized.
16. Internal attacker manipulates the data stream to the high level database, causing a distortion of personal information.
17. Internal or external attacker manipulates data streams from profile maintenance, distorting information in the Difi Database.
18. System error causing the data flows into the databases to be corrupted, distorting database information about users.
19. Customer service accesses personal data for secondary use purposes.
20. Customer service accesses sensitive personal data in the high level database, for secondary use purposes.
21. External attacker wiretaps the customer service phone lines to obtain personal data.
22. External attacker uses phone phreaking vs customer service to obtain personal data about individuals.
23. External attacker exploits the reset password function together with obtained PIN codes to obtain access to accounts.
24. Mobile Phone company documents usage of MinID service, and uses it for surveillance or profiling of customers.
25. Postal service company documents usage of MinID service, and uses it for surveillance or profiling of customers.

9.2.2 Risk Analysis Results

The numbers from the taxonomy of privacy risks is used as measurement of privacy impact (see section 5). Each privacy threat scenario is classified within the taxonomy, and assigned the impact of the most severe risk (some of the threat scenarios have several privacy risks). The numbers used for this analysis, can be seen in figure 17.
The risk analysis can be seen in figure 37. This table is adapted from the tools provided by the Risk IT Practitioners guide. One column called "Time" was removed, and the "Privacy threat" column was added. The frequencies are subjective values determined by the practitioners according to the guidelines of Risk IT.

Scenario nr	Actor	Threat Type	Event	Asset	Privacy threat	Frequen	Frequency comments	Magnitude	Risk Classification
1	External	External Requirement	Inappropriate use	Customers	Insecurity	7	Hacking of Pcs occur daily, and account hijacking is likely to	8,6	Really Unacceptable
2	External	Malicious	Ineffective design	Customers	Secondary use, Function	5	The howto on using this attack is not hidden and is likely to occur	7,9	Unacceptable
3	External	Malicious	Ineffective design	Customers	Insecurity	4	Attack is possible but requires knowledge of vulnerabilities.	8,6	Unacceptable
4	External	Malicious	Interruption	Customers	Exclusion	2	DoS is not likely to occur over a significant time period	8	Unacceptable
5	Internal	Malicious	Inappropriate use	Customers	Insecurity	2	Not a likely target for attack for an insider. Value of target is not	8,6	Unacceptable
6	Internal	Malicious	Ineffective design	Customers	Aggregation	2	Not a likely target for attack for an insider. Value of target is not	6,5	Acceptable
7	Internal/Extern	Malicious	Modification	Customers	Distortion	2	Not a likely target for attack for an insider or	7,5	Acceptable
8	Internal/Extern al	Malicious	Disclosure	Customers	Surveillance	3	Data stream is likely to be encrypted and well secured.	7,7	Unacceptable
9	External	Malicious	Ineffective design	Customers	Insecurity	5	Many mailboxes in Norway lacks security	8,6	Really Unacceptable
10	External	Malicious	Ineffective design	Customers	Surveillance, Denial of anonymity	8	External SP are very likely to have logs of service use, that can be abused outside of Difi's	7,7	Really Unacceptable
11	External	Failure/Natur al	Interruption	Customers	Exclusion	4	Telephony infrastructure is vulnerable for short periods of downtime due to natural disasters	8	Unacceptable
12	External	Malicious	Theft	Customers	Insecurity, Disclosure	2	A likely target for attack, but the database is well protected.	8,6	Unacceptable
13	Internal/Extern al	Malicious	Disclosure	Customers	Insecurity	5	Session hijack is possible through browser weaknesses.	8,6	Really Unacceptable
14	Internal	Malicious	Theft	Customers	Insecurity	7	A likely target for attack by the insider.	8,6	Really Unacceptable

Figure 37: Risk Analysis Risk IT, part 1

Scenario nr	Actor	Threat Type	Event	Asset	Privacy threat	Frequenc	Frequency comments	Magnitude	Risk Classification
15	Internal	Malicious	Ineffective design	Customers	Denial of Anonymity	10	This happens through the use of SSN as identifier	6,9	Really Unacceptable
16	Internal	Malicious	Destruction	Customers	Distortion	2	Not a likely target for attack for an insider.	7,5	Unacceptable
17	Internal/External	Malicious	Destruction	Customers	Distortion	1	Not a likely target for attack for an insider or	7,5	Acceptable
18	Internal	Accidental/Error	Destruction	Customers	Distortion	3	The odd software and hardware errors are likely to occur once in a while	7,5	Unacceptable
19	Internal	Malicious	Disclosure	Customers	Secondary use	5	When the opportunity for abuse of personal data is present, it is likely to be exploited	7,8	Really Unacceptable
20	Internal	Malicious	Disclosure	Customers	Secondary use	4	When the opportunity for abuse of personal data is present, it is likely to be exploited	7,8	Unacceptable
21	External	Malicious	Disclosure	Customers	Insecurity	2	Wiretaps is an unlikely attack vector.	8,6	Unacceptable
22	External	Malicious	Disclosure	Customers	Insecurity	6	Phone phreaking is a low risk, cost effective and common way of attacking	8,6	Really Unacceptable
23	External	Malicious	Ineffective design	Customers	Insecurity	6	This attack does not require intricate knowledge of the system to figure out, and is a	8,6	Really Unacceptable
24	External	Malicious	Ineffective design	Customers	Surveillance, Denial of anonymity	8	Difi have no control of what SP does with the information it recieves. This is an easy accessible source of	7,7	Really Unacceptable
25	External	Malicious	Ineffective design	Customers	Surveillance, Denial of anonymity	4	Difi have no control of what SP does with the information it recieves. But this is a slow	7,7	Unacceptable

Figure 38: Risk Analysis Risk IT, part 2

9.2.3 Use of time

Total time spent on each task and total time use is illustrated in figure 40. A total of 42 hours was spent doing these four tasks, this result will be discussed in chapter 10.

Risk IT, Time use	
Task	**Total hours**
Risk Universe	9
Risk Identification	17
Risk Analysis	12
Complete Report	4
	42

Figure 40: Risk IT total use of time

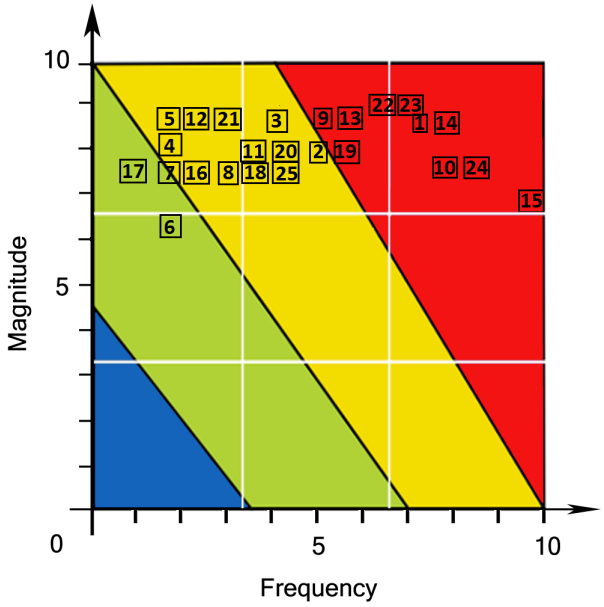


Figure 39: Risk IT, Privacy Threat scenarios

9.3 Summary of Findings using the Risk IT framework

- Risk IT is scoped to detect information security risks, and work must be put in to adapt the framework to detect privacy risks.
- There is no clear risk owner for all the risks. But this can be addressed for the system by the organization taking ownership for all the privacy risks presented by the IdMS.
- Threat modeling yields an abundance of risks for analyzing.
- The majority of privacy risks found using Risk IT and threat modeling were low level risks, many of which were related to system weaknesses.

9.4 Summary of Results using the Risk IT framework

- Total time use was 42 hours.
- 25 Privacy threat scenarios were identified using Risk IT.
- 30 Individual privacy risks were derived from analyzing the privacy threat scenarios.
- Produced a simplified Risk IT report, see appendix B.
- Detected many privacy risks founded in technical vulnerabilities.
- Of the 19 privacy risk classes, Risk IT identified risks within 9 classes.

10 Comparison of Results and Findings from the Case-Studies

This chapter consists of discussions of key findings and results from the two case studies. The chapter is initiated with a general discussion of the two different methods, focusing on advantages and drawbacks of each method. The results from each case study is then presented, compared and discussed.

10.1 PIA findings

According to the PIA framework, a practitioner in our position can conduct a PIA (see section 4.2.1), but the PIA is recommended to be implemented into the project planning process at an early stage. Detecting privacy issues at an early stage will allow the project planners to implement privacy risk reducing measures or to avoid the privacy issues. This fact did not impact the agenda of the PIA case study in this thesis, as the purpose was to uncover risks to privacy in a federated identity management system. The time of detection in the project lifetime is irrelevant to the agenda of this thesis, the purpose is to detect and analyze the privacy risks, and not to implement measures. The advantage of doing the PIA post implementation is that the system is complete, and that it is possible to detect privacy risks present in the system. But it is harder to do anything with the privacy risks when they are already present in the system.

The first thing noticed when using the Internet version of the PIA handbook v2.0, is that it lacks page numbering. The PIA framework uses links within the PDF document to take the practitioner from part to part (and to appendix), this works fairly well as long as the framework remains digital. The different parts and appendices does not give any information about the content in each part, which gives an unprofessional feeling when using the framework. Only the front page of the framework contains an overview of contents, which is very superficial. Implementing a table of content and page numbering would have been a small step for the authors to make a big improvement to the standard. The practitioners in this thesis used a paper copy of the framework (printed from the handbook v2.0 pdf), and found that using the framework without page numbering and a proper table of contents was very frustrating and time consuming. Additional time had to be spent to get to know the framework properly and to make sure that information was not overlooked in the PIA process, this also goes for the digital version of the framework, none of them are easy to grasp or user friendly. The practitioners had to physically browse through the framework to determine its content.
Another small point of critique that adds to the negative impression of the layout of the framework is that the "PIA Decision Tree" figure (see figure 27) contain markings of a spell checker

under the text stating "Full scale PIA" and "Small scale PIA". This may have been done intentionally, but it makes the figure seem less professional.

PIA is classified as an assistant method [11,46], and it tells the practitioners what to do in an orderly fashion. The initial assessment was just as big a task as the other main steps. It is specified that the initial assessment is used to determine which kind of PIA was needed and it did deliver on that account. However, the matter of subjectivity in the screening questions is considered a flaw, and some of the questions may be answered to fit the agenda of the practitioner because of this.
The lack of guidelines when concluding on the initial assessment is also considered a flaw. This is because the framework suggests to answer each of the 11 questions individually, but to conclude on the result as a whole. This also gives the practitioners room to make the scope of the assessment fit their agenda. Having the ability to manipulate the answers from the initial assessment, together with no real guidelines on how to conclude on the answers, is a weak solution at best. I.e. hiring an external consultant at a high hourly wage to do this initial assessment, and single handedly make the decision of conducting the assessment or not, would probably prove to be bad business.
The initial assessment questions are also scoped to be answered in the project start up phase and not post implementation. I.e. Answering the question, "(6) Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?", post implementation could both be answered yes and no. This was because the project did involve both new and significantly changed information handling when it was implemented, but the project had already been up and running for at least three years. Yes, the handling was new when it was implemented, but the solution is no longer new when viewed from a technological perspective. Again, answering such a question is not a simple yes or no for the system (MinID) in question.

The framework provides a very good definition of what privacy is, and why privacy is important. Knowing privacy risks is not always obvious, and PIA supplies the practitioners with basic definitions of privacy risks and what to look for in the detection process. These guidelines are not as extensive as Solove's taxonomy, but they seem adequate in our opinion. The impression of the information regarding privacy in the framework is that it covers the basics well.

A "stakeholder analysis" is not an established term, both stakeholder theory and analysis is fairly new concepts in a scientific contex (first coined by Freeman in 1984 [29]), this term means different things to different people. The purpose of conducting the stakeholder analysis in PIA is not well explained, besides identifying key stakeholders and limiting the amount of stakeholders to fit one page. Stakeholder analysis is too wide a term, amd the approach of case study 1 in this thesis is well within the definition provided in the framework. The only concrete threat identification tool presented in the framework is the initial assessment questions. Aside from this the framework urges the practitioners to consult with stakeholders and a PIA consultation group, one point of critique with this approach is that the framework does not provide any guidelines

on how to conduct interviews to uncover privacy risks. And It does not provide suggestions for suitable risk analysis tools for analyzing privacy risks.

A prevailing issue throughout the framework is that it tells the practitioners what to do, but not how to do it. Which leaves the quality of the conducted PIA more on the shoulders of the practitioners and their chosen approaches. Choosing unfit tools for the job may yield poor results, and the skill of the practitioner will influence the results to a high degree.

10.2 Risk IT findings and comparison

As explained in case study 2, the practitioners had prior knowledge to this framework. This is a more established framework than PIA, but its scope is not specific for assessing risks to privacy. The Risk IT framework [5] and the Practitioner guide [15] both contain page numbering and a table of contents, which sets the first impression of the framework well ahead of PIA. Both of the Risk IT documents seem to have been revised properly before publication.

Contrary to the PIA framework, Risk IT does not provide any specific information on privacy issues or risks. Privacy is mentioned in a couple of sentences within the Practitioner Guide, but is not emphasized. As discussed earlier, risks to privacy are not always obvious and knowledge of the subject is necessary to conduct a privacy risk assessment of high quality using Risk IT. Without knowledge of privacy risks from beforehand, chances are that privacy risks will be overlooked.

Although the data flow diagrams were drawn using a top down approach, a large amount of the identified risks were low level risks, originating in some sort of system vulnerability. In general, the risk identification process using threat modeling, resulted in privacy risks of a technical origin. However, privacy issues are not limited to weaknesses in system architecture and firewalls, and approaching privacy issues with a threat modeling approach may result in not detecting risks that exists between actors in the system. I.e. risks generated by tensions between stakeholders, or by actions conducted by actors in the system who are not regarded as threats or attackers.
With an extensive knowledge of privacy risks, the top-down scenario identification with business objectives in mind might reveal more relevant and realistic risks than using a tool such as DFD. But the quality of the result from this process will be dependent on the subjective expertise of the practitioners.
One of the benefits of the Risk IT and DFD approach is that the same amount of work in risk identification reveals other risks in the system as well, which are not limited to privacy.

10.3 Comparison of results

This section contains a comparison of results based on cost-benefit analysis, using the methodology desecribed in chapter 3. The cost-benefit analysis is presented in the form of time use and

findings. However, the PIA time use must be addressed before conducting the cost-benefit analysis. Because of the time spent creating the PIA report according to the framework, the scope of this thesis was exceeded, and the work hours spent on the PIA reflects this issue. In figure 41 the time use conducting PIA is represented as a whole, but the different processes and their respective results are also represented. The PIA process has been divided into the following phases:

- Full Scale PIA: represents the whole PIA process. Resulting in the complete PIA report.
- PIA, excluding preparation and documentation phase: Represents all PIA activities that are related Risk Analysis. Preparation and documentation phase included activies necessary to produce the PIA report.
- Initial Assessment and Analysis phase: Represents the results from the Initial assessment togehter with the time spent analyzing the detected privacy threat scenarios (Analysis phase).
- Stakeholder Analysis and Analysis phase: Represents the results from the stakeholder analysis, and the time spent analyzing the detected privacy risk scenarios.

10.3.1 Cost-benefit analysis of Time Use

The Risk IT report was created according to the scope of this thesis, and the hours spent on this task did not exceed the scope of the thesis. There was one thing influencing the work hours in the Risk IT process, and that is that the PIA was conducted first. Which means that to conduct the PIA, all the information regarding the MinID system had to be found. At the time when the Risk IT report was written, the practitioners were already familiar with the system, and knew where to look to find the correct information. The scenario description had also been tested in doing the PIA, and had a better quality than when the first case study was conducted. The comparison of the total amount of work hours is therefore recommended to be used only as a guidance for choosing an approach. Figure 41 is a cost-benefit analysis of the different approaches described in this thesis. This figure does not say anything about the importance or quality of the identified privacy threat scenarios or risks, but it reflects the amount of time spent to detect each scenario and risk. Since the MEHARI risk analysis was conducted on both the privacy risks from the Initial assessment and the stakeholder analysis, the work hours have been divided between the two methods by the number risks assessed.

The law of diminishing returns apply to these results; when looking at the results from the stakeholder analysis and MEHARI compared to the PIA (excluding preparation and documentation phase), do the 6 additional detected threat scenarios and the 11 detected privacy risks justify the additional 80 work hours which was used to conduct the initial assessment? And does the additional 115 work hours justify a Full Scale PIA, when compared to a Stakeholder Analysis and Analysis Phase? These are questions future practitioners will have to decide upon. Not conduct-

Method	Work hours	Privacy Threat Scenarios detected	Privacy Risks detected	Additional Gains
Full Scale PIA	187	21	37	PIA Report
PIA, excluding preparation and documentation phase	152	21	37	-
Intial Assessment and Analysis phase	80 (71+9)	10 (6 exclusive)	19 (11 exclusive)	Initial assessment Report
Stakeholder Analysis and Analysis Phase	72 (51+21)	15 (11exclusive)	26 (18 exclusive)	
Risk IT and DFD	42	25	30	Scoped Risk IT report

Figure 41: Cost-benefit analysis of privacy risk approaches.

ing a full scale PIA will have some draw backs, in that the PIA might not be fully integrated into the system development process, and the organization will not get a PIA report at the standard set by the framework.

Full Scale PIA

This approach gave the largest amount of privacy risks. A nice addition to this result was the PIA Report. The full scale was also strong in detecting privacy threat scenarios. However, the biggest drawback of this approach was the amount of work hours used to conduct the full scale assessment.

PIA, excluding preparation and documentation phase

Substracting the hours put into producing the PIA report affects the work hours positively, and does not impact the results. Reducing the amount of work hours by 35, resulting in 152 work hours, 21 scenarios and 37 risks detected.

Initial Assessment and Analysis phase

This process includes only the process of applying the threat identification tool provided by PIA and the time spent analyzing these privacy threat scenarios. This is the weakest approach according the cost-benefit analysis, it costed 80 work hours and resulted in 10 individual privacy risk scenarios, and 19 privacy risks. Of these results an amount, 4 threat scenarios and 8 privacy threats, of both the threat scenarios and privacy risks detected using this tool was redundant when compared with the results from the stakeholder analysis. Leaving the individual contribution of this method at 6 threat scenarios and 11 privacy risks. An addition from this process is the initial assessment report, which gives is used to determine if and what kind of PIA that is

needed, together with an initial assessment of the privacy risks present in the system.

Stakeholder Analysis and Analysis phase

This process resulted in 15 privacy threat scenarios and 26 privacy risk, using 72 work hours. Of these threat scenarios, 4 were also discovered in the initial assessment, togehter with the 8 privacy risks these scenarios produced.

Risk IT and DFD

Risk IT and DFD have by far the lowest time usage, as well as the highest amount of risk scenarios identified, but not the biggest amount of privacy risks detected from this scenario. Even with the fact that this approach was conducted second, and the implications of this on the results, from the cost-benefit point of view, the Risk IT and DFD would still be the best choice. The amount of work hours would have been more if this approach had been conducted first, but it is very unlikely that it would have grown to the scale of the full PIA assessment (152 or 187 hours).
Using DFD gives an abundance of risks to be analyzed in a short time period. With the amount of potential risks the DFD produced, chances are that there are privacy risks that was over overlooked by the practitioners.

10.3.2 Comparison Risk Analysis Results

The two different approaches for detecting risks to privacy differ from each other on what level the risks are detected. Using the PIA and stakeholder approach will result in a high level risk detection by analyzing stakeholder interaction. While using Risk IT and DFD will result in a system specific risk detection. Figure 42 shows risks detected by the two different approaches and their placement in the privacy risk taxonomy (the figure is based on results presented in section 8.1.4 and 9.1.3. PIA totaled 37 privacy risks from 21 threat scenarios, and Risk IT totaled 30 privacy risks from 25 risk scenarios. PIA detected risks within 14 of the 19 risk classifications, while Risk IT detected risks within 9 of the classifications.

Discussion of Risk Analysis Results

Out of the 30 privacy risks detected by Risk IT and DFD, 10 are within the classification "insecurity". This was no surprise as the privacy risk "insecurity" is based on information leakage due to system weaknesses, and DFD is used in information security risk identification for information systems. This is also the most severe risk according to our worst case survey. Risk IT is also strong in detecting "surveillance", "distortion" and "denial of anonymity" risks with 4 of each. 3 instances of potential for "secondary use" was also found. The Risk IT approach detected privacy risks well within 5 classifications of the taxonomy.

	Method 1	Method 2	Risk severity
Privacy Risk	PIA	Risk IT	
1.1 Surveillance	6	4	7,7
1.2 Interrogation	0	0	6,6
2.1 Aggregation	3	1	6,5
2.2 Identification	1	0	8,2
2.3 Insecurity	5	10	8,6
2.4 Secondary Use	2	3	7,8
2.5 Exclusion	0	2	8
3.1 Breach of confidentiality	5	0	8,4
3.2 Disclosure	4	1	8,3
3.3 Exposure	0	0	7,8
3.4 Increased accessibility	1	0	6,6
3.5 Blackmail	1	0	8,3
3.6 Appropriation	0	0	7
3.7 Distortion	1	4	7,5
4.1 Intrusion	0	0	6,4
4.2 Decisional Interferens	1	0	6,2
5.1 Denial of Anonymity	3	4	6,9
5.2 Function Creep	2	1	7,9
5.3 Legal Considerations	2	0	7,8
Total	37	30	

Figure 42: Comparison of results

The PIA process resulted in a diversity of the privacy risks. "Surveillance" were detected 6 times, and represents the privacy risk classification that was detected with highest frequency. Although not as frequent as in Risk IT, "insecurity" was detected 5 times. No instances of exclusion were detected, whereas Risk IT had 2. One big difference between the two methods were that PIA detected 5 potential "breach of confidentiality"-risks and Risk IT did not detect any. This was because of the properties of each risk identification approach, breach of confidentiality happens on the human level, and DFD does not consider stakeholder/human capabilities.

"Disclosure" also holds a difference in result for the same reason, disclosure is leaking harmful personal data about a person, and is a threat with most likely to be initiated with human intent. Both "Disclosure" and "Breach of confidentiality" are risks that have high severity. Although the Risk IT approach found one such threat, this shows that it is difficult to detect risks related to stakeholder capability when using a system specific threat identification tool. Only PIA found risks within "Legal Considerations", this is also a risk with very high severity according to the privacy risk survey. If the legal side of privacy risks is going to be prioritized, doing the legal compliance check and data protection act check is likely to uncover more legal related risks.

10.4 Did PIA live up to expectations?

In this section, the ideal goals from the PIA framework will be discussed briefly. The reason why the PIA report was produced according to the framework, beyond context establishment and risk analysis, was to see if it delivered what it promised as ideal results. What the PIA promises as ideal results is found in section 3.5.

The PIA should deliver an overview of the project's privacy impacts, and it did provide a comprehensive insight into the privacy issues and impacts of the MinID system. The appreciation of those impacts from the perspectives of all stakeholders were not discovered, as the real stakeholders of the project was not involved in this thesis. But the impacts of the capabilities of the key stakeholders were discovered.
It did provide an understanding of the acceptability of the project and its features by the organizations and people affected by it. The project affects over half the Norwegian population, and it was publicly acceptable judging from the amount of users applying the solution. The PIA process also helped identify less privacy invasive alternatives, together with avoidance alternatives (see the PIA reort appendix A. The business case and justification for privacy intrusive measures was identified as a part of the PIA process, and documented in the PIA report.
All in all, the PIA did deliver on almost all accounts of what it promised. But the result of this process may vary, as choice of tools and available time, togehter with uncertainty in the initial assessment may influence the PIA process.

10.5 Summary, Comparison of key findings

PIA:

- The PIA should be implemented as a part of the project planning process, as privacy risks detected pre implementation are easier to deal with.
- The PIA Handbook v2.0 pdf lacks page numbering and a table of contents, which makes using the framework cumbersome to work with, and gives an unprofessional impression.
- The PIA provides exstensive and covering information regarding privacy risks and what to look for.
- The use of adjectives in the initial assessment questions, combined with the lack of guidelines for how to conclude on the assessment will allow all non-extreme results to be manipulated to fit the agenda of the practitioners.
- Stakeholder Analysis is not an established term, and the purpose of conducting a stakeholder analysis, beyond compiling a one page list of stakeholders for interviews, in PIA is unclear.
- PIA does not provide any guidelines on how to conduct interviews with stakeholders and the PIA consultation group in order to uncover privacy risks.

- The quality of the PIA report will be very dependent on the skills of the practitioners conducting the assessment, due to lack of guidelines on how to solve tasks and choose tools for the job.

Risk IT:

- Risk IT lacks definitions of what privacy and privacy risks are, since the scope of the approach is classical information security.
- Risk IT provides definitions of all the risk-related terms used in the framework.
- Has pagenumbering and table of contents, and a professional look.
- Requires prior knowledge of privacy risks to be used for privacy risk detection.
- Using Risk IT and threat modeling for privacy risk analysis is probable to results in a large amount of risks related to technical vulnerabilities.
- The same amount of work conducting threat modeling, will also reveal risks that are not exclusive to privacy risks.

10.6 Summary, Comparison of results

Cost-benefit analysis:

- Full Scale PIA was had the largest number of privacy risks detected, but also took the longest to carry out.
- Risk IT and DFD had by far the lowest time usage, as well as the highest amount of risk scenarios identified.
- From the cost-benefit point of view, the Risk IT and DFD seems the best choice. While Stakeholder analysis and together with MEHARI was the second best.
- When compared to the Stakeholder Analysis, the initial assessment of the system only resulted in 6 individual privacy threat scenarios and 11 privacy risks, because of overlap in risk identification. The time use of this process was 80 work hours. While the stakeholder analysis resulted in 15 privacy threat scenarios and 26 privacy risks, by 72 hours of work.
- Risk IT and DFD produced a large amount of system specific risks on a relative short period of time.
- Stakeholder analysis also produced a large amount privacy risks, but over a longer time span.
- The Initial assessment was the process that resulted in least results according to the cost-benefit analysis.

Results from the Risk Analysis:

- PIA detected privacy risks of a larger diversity, since the scope of this approach focuses on the stakeholders within in the system, and their interactions. In total PIA detected risks within 14 of the 19 privacy risk classes, and Risk IT detected risks within 9 of them.
- A large amount of the risks found by Risk IT were system related, and withing the classification "insecurity", which is founded in software and hardware vulnerabilities and data leakages.
- Risk detected two risks of the class "Exclusion", and PIA detected none.
- Risk IT was not able to detect any privacy risks within the classes "Breaches of Confidentiality" and "Legal Considerations", while PIA detected risks in both categories.
- Risk IT was weak in detecting risks within the class "Disclosure", whereas PIA were stronger.
- Risks within the classifications "Interrogation", "Appropriation", "Exposure" and "Intrusion" was not detected in the MinID system.
- Likely to miss privacy risks founded in tensions between actors in the system, or privacy risks generated by actions of actors not regarded as attackers, and threats found in non-compliance with law.

11 Discussion

In this chapter the results obtained throughout this thesis are discussed, together with a discussion on how these results relate to the research questions presented in chapter 1.

11.1 Research Question 1

A comparison of the two risk management approaches "Privacy Impact Assessment" and "The Risk IT Framework" has been presented in this thesis. This comparison was conducted using a comparative case study, with both qualitative and quantitative approaches. Based on the PIA initial assessment, a full scale PIA was conducted on the system, while the Risk IT process consisted of defining a risk universe and risk analysis.
The general impression of the PIA framework, when compared to Risk IT, is that PIA is a more cumbersome approach privacy risk assessment. This is because of the many problems and lack of information within the framework. A prevailing problem in the PIA Initial Assessment is the use of adjectives, which allows for interpretations by the practitioners. This presents problems when conducting the initial assessment of the system, as it is not obvious what the question is asking due to lack of definitions. And it presents a weakness as the questions can be answered to fit agenda of the practitioner which could have been avoided by rephrasing the questions.together with the lack of definitions, the use of non-established terms is also a problem in the framework. The PIA does provide definitions of privacy (and why it is important), privacy risks (and what to look for), and privacy strategies, but it is hidden in a framework that does not provide a table of contents and even lacks page numbering. It also lacks information on what to do when conducting a "stakeholder analysis" and what steps to take when conducting a "risk analysis". The goal of the risk analysis in PIA is to "Identify the design issues and privacy problems with the project" [4], but this is as far as guidance goes. A solution to this problem i.e. would have been add some recommendation privacy risk tools, or add more extensive guidance on how to choose a tool for the risk analysis.
Another problem related to guidance is that the framework does not provide any concrete advice on how to conclude on the initial assessment. The sentence: "Once each of the 11 questions has been answered individually, the set of answers needs to be considered as a whole, in order to reach a conclusion as to whether a full-scale PIA is warranted" [4], is the only guidance provided for concluding on the initial assessment. Since all the 11 questions can be answered "yes" and "no", a more concrete guideline could have been easy to implement.
Not defining the term "Stakeholder Analysis" is not the only problem regarding stakeholders. The framework does not provide sufficient guidelines on how to undertake a stakeholder anal-

ysis and what this includes. It does provide guidelines for stakeholder identification, and that the result from this process should ideally be one page summary of stakeholders and their stakes in the project. The reason why Risk IT is regarded as a more structured and easy-to-follow approach to risk management, is that it is a standard that has a layout which is easy to follow and comprehensible, it also provides definitions of terms used in the framework. The process of risk identification and analysis is well described in Risk IT, using both text and figures for illustration (see figures 15 and 16). The way the information is structured and presented is significant in this process. Our impression is that Risk IT have been prepared thoroughly before release, while PIA has many flaws (due to lack of structure in the document) and is not comprehensive while being a time consuming approach.
There are drawbacks of choosing PIA, which have already been mentioned, but there are also advantages. When it comes to privacy, PIA provides comprehensive background information about the subject, where Risk IT does not provide any information. The Risk IT framework is not specifically scoped for privacy risk detection. The framework does not address privacy, or risks to it, as a particular issue. Risk IT must therefore be adapted to work for privacy risk detection, this problem was solved in this thesis by using the privacy risks presented in chapter 5. Using a more established approach to risk assessment would require the practitioners to acquire background information regarding privacy risks to be successful. While PIA provides its own definition of privacy risks, together with some guidelines on how to recognize them. The PIA framework also provides step-by-step plans on how to conduct the PIA process.

During the comparison it was found that conducting PIA is a time consuming approach with a total of 187 work hours. Even when the work that was conducted solely for the purpose of producing the PIA report was subtracted, the total amount of work hours were 152, which is 110 more than the familiar approach of Risk IT (42 hours). The Risk IT approach uncovered 25 privacy threat scenarios and 30 privacy risks. While PIA uncovered 21 individual privacy threat scenarios, and 37 privacy risks.
Conducting this comparative case study using an identical scenario may have impacted the cost-benefit analysis more than anticipated. There is no doubt that conducting the PIA is a more time consuming approach, but it used almost 4 times more work hours than conducting PIA, which is a result that is likely to be heavily influenced by already knowing the system for case study 2. Familiarity with the system and the issues identified in case study 1, did also act as a time reducing factor for case study 2 in modeling the system. It is certain that modeling the DFD would have taken longer time if the PIA was not conducted first.
A limitation of 2 privacy risks per threat scenario was also set, some of the threat scenarios may present more risks than two. Discovering privacy risks in some of these threat scenarios may only be limited to imagination of the practitioners, so putting two as a limit on each scenario is a limitation, but it also helped the practitioners emphasize the two most important for the scenario.

Impact and the probabilities presented in the two case studies may not reflect realistic values, as the PIA probability values were obtained using open sources and the stakeholder analysis

method presented as a part of this paper. The privacy impact results for PIA was gathered from the survey conducted in this thesis (see Appendix E for the survey and Chapter 5 for results). For Risk IT, the same survey results was used for impact, together with an estimate of probability conducted by the practitioners. The final risk values was weighted on "High" and "Very High" for both the case studies, this result was heavily influenced by the worst case survey results, which ranked all the risks between 6-9 on the impact scale. It is very likely that the final results of the risk analysis would be "nicer" if the impact was estimated as worst-case for Difi and not for the user, as Difi would probably not mind privacy risks as long as there is no likelihood of the privacy risk impacting them financially. The probabilities may also have been adjusted to be lower if documentation about the security measures within the system were available.
In this thesis the side of the individuals are considered when evaluating risks to privacy (category 1 of PIA definition [4]). This angle may be hard to sell to most organizations, as they are likely to care less about the rights of individuals and more about how the risk can harm their reputation or financially. This perspective was also chosen as a consequence of using open sources, it would provide too much guesswork to estimate financial damage to organization based on privacy risks.
The questionnaire used to determine privacy impact to the individuals was also too simple to determine realistic values for privacy impact. The survey was created as a worst case for each privacy risk classification to fit both risk analysis, as previously mentioned, the results reflect the worst case angle. This was a weakness because it is not always possible for the identified privacy risk scenarios to develop into the worst case scenario depicted in the survey. The results from the survey also reflect that it is worst-case.

11.2 Research Question 2

The second research question asked how to use stakeholder analysis to detect privacy risks in IdMS. The developed methodology of using stakeholder analysis for threat identification is presented in chapters 4 and 6, where the stakeholder definitions provided by Mitchell et.al. [12] and Freeman [29] were used, and the methodologies presented by McManus [30] (recommended by Pacheco and Garcia [32]) and Schmeer [41] formed the foundation for the stakeholder analysis. The stakeholders were chosen from their importance and influence in the project. The information needed to detect privacy risks in the IdMS was determined through trial and error, and using relevant literature [12, 30, 35, 41, 52, 53, 55].
The stakeholders and their attributes were determined through analyzing stakeholder capabilities. The consequence of the capability were determined for the assets, the effect for the stakeholder, and how the consequence affected other stakeholders. Privacy was regarded as an asset (property), and if the capability affected an asset negatively, a potential privacy threat scenario was identified. Further experiments will have to be conducted to determine if the stakeholder analysis method described in this thesis is transferable to a real life setting. Conducting the stakeholder analysis based on open sources only will not give a realistic picture of the stakeholder attributes and their evaluation of assets and relationships. Interaction between the practitioners

and the stakeholders are required to determine the attributes and their values.
A method for utilizing the stakeholder attributes in probability calculation was also presented in chapter 6. This method was adapted to fit the residual likelihood calculation in MEHARI [14], where the knowledge level, relationships between the stakeholders and impact on assets were used to calculate residual likelihood. To determine validity and applicability of the results from this method require further experiments should be conducted. Unless there has been a significant change in circumstances, the best approach for calculating likelihood is to apply historical data. Because of this, the likelihood method suggested in this thesis should be experimented with further where no such data is present, and compared to other approaches developed for likelihood calculation for such circumstances.

11.3 Research Question 3

To answer research question 3, the stakeholder analysis methodology described in research question 2 is compared to a more established threat identification tool. Both these tools were integrated into the case studies, the stakeholder analysis is a part of the PIA process, while threat modeling were used in case study 2, the results are presented in chapters 8, 9 and 10.
The literature for using threat modeling as a privacy risk identification tool is presented in chapter 2 (see [34, 35]), and is founded upon dataflow diagrams (see [33]. Together with the traditional CIA, an additional column was added to the analysis to scope this tool for detecting privacy threats. This column was a simple "yes" or "no" if the detected risk was privacy related. This is why prior knowledge about privacy risks are required for using this tool, or else the practitioners will not know what to look for, and how the risk can relate to privacy. The comparison of these two tools uncovered that the stakeholder analysis identified 15 privacy threat scenarios, and threat modeling uncovered 25 privacy threat scenarios. The stakeholder analysis was conducted in 51 hours, and the threat modeling was conducted in 17 hours. Threat modeling resulted in a larger amount of privacy threat scenarios in a shorter amount of time.
The results from analyzing risks detected from the stakeholder analysis, showed a higher diversity than the threats identified using threat modeling and Risk IT. The stakeholder analysis alone identified risks within 12 out of the 19 risk classifications, and together with the scenarios from the initial assessment, the amount was 14 out of 19. Risk IT detected risks within 9 of the 19 classes.The amount of privacy risks detected was 26 identified using stakeholder analysis, and 30 identified using threat modeling. Out of the 30 detected by threat modeling 10 were classified within "Insecurity", which shows that using threat modeling will result in more system specific privacy risks. Using this approach may result in the practitioners overlooking risks that are found at a higher level in the organization. While the stakeholder analysis will be founded in interactions between stakeholders, and their capabilities. PIA is also capable of detecting risks within the "insecurity" classification, but not as strong as Risk IT, potential system specific privacy risks may be overlooked using PIA.
The Risk IT findings being weighted on "Insecurity" raises the question of how suitable the threat modeling approach was for detecting risks to privacy. As this methodology does require prior

knowledge of privacy risks and modification of identification process to increase usability. Another tool scoped for detecting privacy risks may have been better suited for the comparison, but additional time would have been required to get to know and use a new tool, and these resources was not available.
Limitations was also set on both threat identification approaches, the stakeholder analysis was limited to eight stakeholder classes, while the DFD models were kept on a superficial level and limited to two models for analysis. Both the stakeholder analysis and the DFD have the potential to uncover more privacy risk scenarios, but due to time restrictions and complexity, it was put limitations on both the PIA and the Risk IT when identifying privacy threat scenarios for analysis.

11.4 Research Question 4

This question was which risks within the privacy risk classification was found in MinID IdMS. To answer this question, the findings from the two case studies were addressed. The risk analysis conducted in this project showed that out of 19 privacy risk classifications, there were detected risks within 15 of them combining the results from both approaches. Risks within the classifications "Interrogation", "Appropriation", "Exposure" and "Intrusion" were not detected in the MinID system using the methodologies presented in this project. This does not mean that there is not a possibility for the risks existing within identity management systems, but it does mean that the practitioners conducting the two risk assessments were unable to detect them in MinID.
The PIA process resulted in detection of risks within 14 of the 19 privacy risk classes, which is interpreted as a good result for detecting privacy risks. The majority of these risks were found using the stakeholder analysis, which together with the initial assessment detected 37 privacy risks. The results from these two processes within PIA overlapped to some degree, and the threat identification results from the stakeholder analysis had a better result than the initial assessment. Risk IT detected privacy risks within 9 of the 19 privacy risk classes, where risks within one class ("Exclusion") was detected exclusively by Risk IT. Which is interpreted as a good result for detecting privacy risks. The majority of these risks were found using the stakeholder analysis, which together with the initial assessment detected 37 privacy risks. The results from these two processes within PIA overlapped to some degree, and the threat identification results from the stakeholder analysis had a better result than the initial assessment. Risk IT detected privacy risks within 9 of the 19 privacy risk classes, where risks within one class ("Exclusion") was detected exclusively by Risk IT.

What was not compared in the case study, was similarity in the privacy risk scenarios detected. Time limitations did not allow for this to be conducted, but this would have given an insight to where in the system the different risks were found, and if the two methods detected the same risks.

12 Future work

In this chapter possible future work is presented based on the findings made during the process of conducting this master's thesis. The suggested work is related to the main topics covered; IdM, privacy, privacy risks, stakeholder analysis and risk analysis.

- A comparison of the two approaches in a more objective environment is suggested. Such as, conducting the two approaches on an IdMS using two different practitioners of equal skill, to obtain a more objective result.
- Another suggestion for further work is regarding the execution of the Privacy Impact Assessment. Implementing the PIA in the starting phase of a project may yield better results regarding detection of privacy risks. And conducting the PIA with emphasis on risks to the organization, instead of the individual, will be a more valid approach as organizations are likely to be concerned with how a privacy risk can impact them. A comparison of performance conducting the PIA pre- and post-implementation can also be used.
- A comparison of privacy risk assessment frameworks and tools where the specific risks are considered, i.e. did the approaches detect identical risks located within the same locations in the system, and how are they analyzed? This can be used to determine strong approaches to privacy risk analysis.
- Conduct the PIA privacy law and the Data Protection compliance checks to see if these uncover any additional risk to privacy, and evaluate the additional value these two checks add to the process.
- Conduct further tests using the stakeholder analysis as a means to detect privacy risks. The method needs to be tested on a more complex system with more stakeholders. More details can also be added to the analysis to better predict situations where privacy may be at risk. Interviews and surveys can be employed to map and evaluate the stakeholder attributes, this work can help formalize the method for future use. The likelihood determined for each stakeholder capability is also a subject for further research, a comparison of this method and a more established method for likelihood calculation can be conducted.
- Further work within the field of privacy risks. In this thesis 19 privacy risk classes were used, there are probably more risks to add to the classification. The impact of these risk classifications can also be mapped to a larger extent.
- A future study of privacy risks in IdMS can also be conducted to help determine within which

of the privacy risk classifications risk are commonly found in such system, as an indicator to help practitioners determine what to look for and where to look.

- Threat modeling was a cost efficient approach, and further development of this approach for detection of privacy risks is suggested. Such as combination of tools such threat modeling and stakeholder analysis.

13 Conclusion

This chapter contains the final conclusions with regards to the research questions presented in this thesis.
The Privacy Impact Assessment is an approach that can be used without prior knowledge to privacy risks. While Risk IT requires extra research to be used for the purpose of privacy risks. The PIA framework requires the practitioners to use their own tools scoped for stakeholder and risk analysis, no standardized stakeholder or risk analysis tools leaves the quality of the assessment more on the shoulders of the practitioners. Risk IT provides tools for the risk assessment process, but the tools provided need adjustments to be used as privacy risk assessment. The Risk IT framework is more comprehensive and easier to work with than the Privacy Impact Assessment used in this thesis. As the PIA Handbook v2.0 lack page numbering and a table of contents. PIA defines terms regarding "Privacy" and "Privacy Risks" well, but besides from this, it lacks term definitions and recommendation of tools. Following the PIA framework and writing the PIA report as specified in the framework was also a time consuming approach. Risk IT is a more mature framework than PIA, but it requires prior knowledge of privacy risks to used for privacy risk assessment purposes. PIA is not easy to use and the practitioners have to choose their own tools for stakeholder and risk analysis, but it provides guidance for "privacy" and can therefore be used without prior knowledge of the subject.
Judging from the cost-benefit point of view, the Risk IT and DFD approach seems the better approach, as case study 2 was conducted in a third of the time spent conducting PIA. The Risk IT approach yielded an abundance of threat scenarios to be analyzed in a short period of time, resulted in a large amount of privacy risks present in MinID. The PIA process resulted in fewer privacy threat scenarios, but the analysis of these scenarios resulted in a larger number of privacy risks for MinID. From a cost-benefit point of view, the Risk IT framework is therefore the superior choice of approach.
The stakeholder analysis methodology presented in this thesis, was scoped for detecting risks to privacy in IdMS. It was mainly based on related work (see chapters 4 and 6). To use stakeholder analysis for privacy threat detection, the stakeholder's capabilities, assets and relationships to other stakeholders was mainly used. Every capability that could impact privacy of the users were analyzed. The method yielded good results in case study 1, 15 privacy threat scenarios in 72 work hours (51 excluding risk analysis of each scenario). Although the stakeholder analysis approach seemed successful in this thesis, it still needs to tested in other scenarios to further determine usefulness for other IdMSs'. The stakeholder analysis methodology used for privacy threat identification was successful in this thesis, but it needs more experimenting to verify validity.
Threat modeling was the tool chosen for comparison to stakeholder analysis. Threat modeling was integrated into case study 2, and threat modeling resulted in a large amount of potential

risks to be analyzed. To limit the amount of potential scenarios, risks that had contained no obvious risk to privacy was left out of the analysis. The PIA case study resulted in more high level risks, related to stakeholder interactions and capabilities. While the Risk IT approach used in this thesis resulted in more system specific risks. PIA also detected system specific risks, but not to the same degree as Risk IT. The Privacy Impact Assessment results in a larger number of risks with higher diversity, but the process is not cost-effective regarding work hours. Risk IT detects a large amount of privacy risks in a shorter period of time and is very cost effective, but does not detect privacy risks with the same diversity as PIA.
After analyzing the privacy threat scenarios detected in both case studies, privacy risks within 15 of the 19 privacy risk classifications by Solove [6] and PIA [4] was detected in the IdMS of this thesis. Risks within 14 of the 19 classes was detected using PIA, and risks within 9 of the 19 classes was detected using Risk IT.

Bibliography

[1] Zalta, E. N., Nodelman, U., Allen, C., & Perry, J. 2006. Stanford encyclopedia of philosophy; privacy. (Visited Nov. 2011).

[2] Minid - your public id. http://minid.difi.no/minid/minid.php?lang=en. (Visited Mar. 2012).

[3] 2012. Om difi. http://www.difi.no/om-difi.

[4] 2009. Privacy impact assessment handbook version 2.0.

[5] ISACA. 2009. The risk it framework.

[6] Solove, D. J. 2006. A taxonomy of privacy. *University of Pennsylvania Law Review*, 154, 477–558.

[7] 2008. Iso/iec 27005 - information security risk management.

[8] Hansen, M., Borcea-Pfitzmann, K., & Pfitzmann, A. 2005. Prime - ein europäisches projekt für mutzerbestimmtes identitätesmanagement. *Information Technology, Oldenbourg*, 6(47).

[9] Srinivasan, M. K. & Rodrigues, R. 2010. Analysis on identity management systems with extended state-of-the-art idm taxonomy factors. *International Journal of Ad Hoc, Sensor & Ubiquitous Computing*, 1(4), 62–70.

[10] Pashalidis, A. & Mitchell, C. J. 2003. *A Taxonomy of Single Sign-On Systems*. Springer-verlag Berling Heidelberg.

[11] Campbell, P. L. & Stamp, J. E. 2004. *A classification scheme for risk assessment methods*. Sandia National Laboratories.

[12] Mithcell, R. K., Agle, B. R., & Wood, D. J. 1997. Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts. *The Academy of Management Review*, 22(4), 853–886.

[13] ENISA. 2006. Inventory of risk assessment and risk managemnet methods. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/inventory-of-risk-assessment-and-risk-management-methods.

[14] 2010. Mehari 2010 - risk analysis and treatment guide. http://www.clusif.asso.fr/.

[15] ISACA. 2009. The risk it practitioner guide.

[16] Westin, A. 1967. *Privacy and Freedom*. New York: Atheneum.

[17] Rachels, J. 1975. Why privacy is important. *Philosophy & Public Affairs*, 4(4), 323–333.

[18] 2000. Personal data act. `http://www.lovdata.no/all/hl-20000414-031.html`. (Updated 2009).

[19] 2001. Personal data regulations. `http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20001215-1265.html`. (Updated 2010).

[20] Garfinkel, S. 2000. *Database Nation; The Death of Privacy in the 21st Century*. O'Reilly & Associates, Inc.

[21] Paintsil, E. & Fritsch, L. 2011. A taxonomy of privacy and security risks contributing factors. *IFIP Advances in Information and Communication Technology*, 352, 52–63.

[22] Gross, J. B. & Rosson, M. B. 2007. *End User Concern about Security and Privacy Threats*. The Pennsylvania State University.

[23] Zalta, E. N., Nodelman, U., Allen, C., & Perry, J. 2002, revised 2010. Stanford encyclopedia of philosophy; personal identity. (Visited Nov. 2011).

[24] Zalta, E. N., Nodelman, U., Allen, C., & Perry, J. 2004, revised 2009. Stanford encyclopedia of philosophy; identity. `http://plato.stanford.edu/entries/Identity/`. (Visited Nov. 2011).

[25] Pfitzmann, A. & Borcea-Pfitzmann, K. 2009. *Lifelong Privacy: Privacy and Identity Management for Life*. Technische Universität Dresden.

[26] 2009. Iso 31000.

[27] Wright, D. 2011. Should privacy impact assessments be mandatory? *Communications of the ACM*, 54(8), 121–131.

[28] Syalim, A., Hori, Y., Kouchi, & Sakurai, K. 2009. Comparison of risk analysis methods: Mehari, magerit, nist800-30 and microsoft's security management guide. *International Conference on Availability, Reliability and Security*, 726–731.

[29] Freeman, R. E. 1984. *Strategic Management: A Stakeholder Approach*. Cambridge University Press.

[30] McManus, J. 2004. A stakeholder perspective within software engineering projects. *Engineering Management Conference, 2004. Proceedings. 2004 IEEE International*, 2, 880–884.

[31] 1996. *The World Bank Participation Sourcebook*. The World Bank.

[32] Pacheco, C. & Garcia, I. 2009. Effectiveness of stakeholder identification methods in requirements elicitation: Experimental results derived from a methodical view. *IEEE/ACIS International Conference on Computer and Information Science*, 8, 939–942.

[33] Bruza, P. & van der Weide, T. 1989. The semantics of data flow diagrams. *Proceedings of the International Conference on Management of Data*.

[34] Burns, S. F. 2005. Threat modeling: A process to ensure application security. *Sans Institute InfoSec Reading Room*.

[35] Swiderski, F. & Snyder, W. 2004. *Threat Modeling*. Microsoft Press.

[36] Moore, R. E. 1966. *Introduction to Interval Analysis*. SIAM.

[37] Caves, C. M., Fuchs, C. A., & Schack, R. 2002. Quantum probabilities as bayesian probabilities. *Phys. Rev. A*, 65, 022305.

[38] Leedy, P. D. & Omrod, J. E. 2010. *Practical Research - Planning and Design*. Pearson Educational International.

[39] Zalta, E. N., Nodelman, U., Allen, C., & Perry, J. 2006. Models in science.

[40] Flyvbjerg, B. 2011. *'Case Study' in Norman K. Denzin and Yvonna S. Lincoln's The Sage Handbook of Qualitative Research*. Thousan Oaks, CA.

[41] Schmeer, K. 2009. Stakeholder analysis guidelines. *Washington DC: Section 2 of Policy Toolkit for Strengthening Health Reform*.

[42] 2011. Minid - sikkerhet og personvern. `http://www.difi.no/elektronisk-id/minid/sikkerhet-og-personvern`.

[43] 2006. Offentlighetsloven. `http://www.lovdata.no/all/hl-20060519-016.html`. (Updated 2011).

[44] 2012. Sikkerheit og funksjonalitet. `http://www.difi.no/artikkel/2011/11/sikkerheit-og-funksjonalitet`. (Visited feb 2012).

[45] 2010. To millioner kan legge bort pin-kodene. `http://www.difi.no/artikkel/2010/04/to-millioner-kan-legge-bort-pin-kodene`. (Visited Feb. 2012).

[46] Abu-Nimeh, S. & Mead, N. R. 2010. Privacy risk assessment in privacy requirements engineering. *Second International Workshop on Requirements Engineering and Law*, 17–18.

[47] 1970. Forvaltningsloven (governance act). `http://www.lovdata.no/all/hl-19670210-000.html`. (Updated 2010).

[48] 2004. Lov om elektronisk kommunikasjon (act of electronic communications). `http://www.lovdata.no/all/hl-20030704-083.html`. (Updated 2008).

[49] 1948. The universal declarations of human rights. `http://www.un.org/en/documents/udhr/`.

[50] Gillom, J. 2001. *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy 3*. Chicago Series in Law and Society.

[51] Posner, R. A. 1999. *The Problematics of Moral and Legal Theory*. Harvard Law Review.

[52] Pipkin, D. L. 2002. *Halting the Hacker: A Practical Guide to Computer Security, Second Edition*. Prentice Hall.

[53] Audestad, J. 2009. *E-Bombs and E-Grenades: The Vulnerability of the Computerized Society*. HiG.

[54] 2001. Identify stakeholders. http://web.mit.edu/urbanupgrading/upgrading/issues-tools/tools/Ident-stakeholders.html. Stakeholder method by ZOPP and NORAD (Visited April 2012).

[55] Johnson, W. H. 1999. An integrative taxonomy of intellectual capital: measuring the stock and flow of intellectual capital components in the firm. *International Journal on Technology Managment*, 18, 562–575.

[56] Ølnes, J. 2012. Evolution of minid and the id portal, lecture. https://wiki.uio.no/mn/ifi/AFSecurity/index.php/Main_Page. Lecture held in UiO, 250112, AF Security.

[57] 2010. Kravspesifikasjon for pki. http://www.difi.no/artikkel/2010/04/kravspesifikasjon-for-pki. (Visited Feb. 2012).

[58] 2010. Kravspesifikasjon for pki i offentlig sektor, versjon 2.0. http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/2010_Kravspek_PKI_norsk.pdf. (Visited Feb 2012).

[59] D-nummer. http://www.skatteetaten.no/no/Alt-om/Folkeregistrering/D-nummer/. (Visited Feb 2012).

[60] 2012. Virksomheter som benytter id-porten. http://www.difi.no/artikkel/2011/05/virksomheter-som-benytter-id-porten. (Visited Feb. 2012).

[61] 2010. Sikkerhet og personvern. http://www.difi.no/elektronisk-id/sikkerhet-og-personvern.

[62] Privacy and security. http://minid.difi.no/minid/personvern.php?lang=en. (Visited feb 2012).

[63] October 2011. Brukermanualer (user guides). http://www.difi.no/artikkel/2010/11/brukerguider-minid. (Visited April 2012).

[64] 2005. enorge 2009. http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eNorway_2009.pdf. (Visited Feb 2012).

[65] 2006-2007. Stortingsmelding nr 17, eit informasjonssamfunn for alle.

[66] 2008. Rammeverk for autentisering og uaaviselighet i elektronisk kommunikasjon med og i offentlig sektor. http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID_rammeverk_trykk.pdf. (Visited Feb 2012).

[67] 2011. Informasjon om sikkerhetsnivå. http://www.difi.no/artikkel/2010/11/informasjon-om-sikkerhetsnivaa. (Visited Feb. 2012).

[68] 2001. E-signature act. http://www.lovdata.no/all/hl-20010615-081.html. (Updated 2005).

[69] 2004. E-gorvenance regulations. http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20040625-0988.html. (Updated 2009).

[70] Østvold, B. M. 2010. Case study - privacy-relevant information flow in information management systems. http://petweb2.projects.nislab.no.

[71] Oasis security services (saml) tc. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security. (Visited Feb. 2012).

[72] Openam. http://forgerock.com/openam.html. (Visited March. 2012).

[73] Open directory service. http://www.opends.org/. (Visited March. 2012).

[74] 2011. Difi - organisasjonskart. http://www.difi.no/om-difi/organisasjonkart. (Visited april 2012).

A Appendix - Privacy Impact Assessment Report

Privacy Impact Assessment Report

Gaute B. Wangen

2012/06/31

Abstract

This Privacy Impact Assessment (PIA) was conducted as a deliverable of the master's thesis "Risk Analysis for Privacy and Identity Management", which was carried out at Gjøvik University College spring semester 2012. The framework that was followed in this project was the "Privacy Impact Assessment Handbook v2.0" provided by the Information Commissioner's Office UK. The identity management system (IdMS) assessed in this report was "MinID", which was provided by the Norwegian Agency for Public Management and eGovernment (Difi)[1].

The risk identification method adapted for this project was stakeholder analysis, and the risk analysis method used was MEHARI[2]. The PIA framework was followed as strictly as possible to obtain the best possible basis for comparison. The type of PIA conducted was a full scale system specific assessment. Although a part of the full scale assessment, the privacy law compliance and data protection act compliance checks were not conducted as a part of this assessment.

This report contains an introduction to project goals and report outline, an introduction to the MinID IdMS, a Risk Analysis, and a discussion of results, possible privacy strategies and reduction measures.

Contents

1 Introduction

This report is a result of following the Privacy Impact Assessment(PIA) Handbook v2.0[3] (referred to only as the Handbook or PIA, in this document). The privacy impact assessment has been conducted on a scenario based on an identity management system (IdMS). The PIA presented in this report was a full scale assessment, but leaving out the Privacy Law and the Data Protection Act compliance check, as these two was outside of the project scope (for more information see section 2.2).
The PIA was conducted as a part of a master's thesis, and the initial purpose of the assessment is to help increase understanding of privacy risks in IdMS. It was also conducted to measure if the PIA delivers what it promises, since it is specific for privacy risks when compared to other risk assessment methods.

1.1 Project Goals

The main goal of this project was to successfully conduct a correctly scaled PIA on the Norwegian Agency for Public Management and eGovernment's (Difi) MinID identity management system. If the PIA is completed to a certain degree of satisfaction, the ideal results according to the Handbook can be:

1. the identification of the project's privacy impacts;
2. appreciation of those impacts from the perspectives of all stakeholders;
3. an understanding of the acceptability of the project and its features by the organizations and people that will be affected by it;
4. identification and assessment of less privacy-invasive alternatives;
5. identification of ways in which negative impacts on privacy can be avoided;
6. identification of ways to lessen negative impacts on privacy;
7. where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them;
8. documentation and publication of the outcomes.

These ideal results are used as project goals and performance indicators on how well the PIA delivered in our case study.

1.2 Report Outline and Appendices

This report has the following structure:

1. Introduction: Short introduction to why the PIA was conducted.
2. The MinID Identity Management System: Presentation of the IdMS, goals of the system,, features, summary of the initial assessment, and the stakeholders of the system.
3. Risk Analysis: Presentation of the identified threat scenarios in the system, and an analysis of the threat scenarios.
4. Discussion of the Results: Contains the business rationale for using privacy intrusive technologies, discussion of chosen privacy strategy, and suggestions for risk mitigating measures.

The report also have the following appendices

1. Appendix 1 - The Initial Assessment: the initial assessment of the system with answered screening questions, and an initial assessment of privacy risks.
2. Appendix 2 - The PIA Project Plan: completed and attached to the report as recommended by the handbook.
3. Appendix 3 - Malicious Actions Mapped by Stakeholders: A stakeholder representation of actions that can threaten privacy in the system.

2 The MinID Identity Management System

In 2005, the Norwegian government published a document called "eNorway 2009"[4], which together with "‘Stortingsmeldingen nr 17"[5] form the basis for the government’s goal of digitalizing the public services in Norway. One of the main purposes of this was to increase efficiency is public services, and moving from paper based services to digital public services was essential. Difi is a governmentally owned organization, and their vision is "We develop the public sector"[1]. Difi aims to contribute to the public sector by renewing and developing it, and strengthen cooperation between vendors and offer joint solutions.
According Difi’s website[6], the system handles privacy related information, and Difi acts as a controller of the personal data handled by MinID. It holds the user’s Norwegian social security number (SSN), and PIN-codes. Difi also logs information about the user’s MinID use. The information kept in the user profile is mobile phone number and/or e-mail address, which is used to administrate MinID.

2.1 MinID system description

The Norwegian Agency for Public Management and eGovernment (Difi) has a mandate to establish a common infrastructure for using electronic identities in the Norwegian public sector[7]. Requirements for a Public key infrastructure(PKI)[8] in Norway was published in 2005 (later updated in 2010), which forms the foundation for the common infrastructure in Norway. Difi has created the solution MinID, which is an identity management system, providing Norwegian citizens with their own personal electronic identity based on their social security number (birth number). MinID can be used to log in to a single access point, called the "ID-portal", which facilitates access to a wide range of available public services[1]. MinID is currently one out of three available solutions for logging in to the ID-portal.
Transparency is important to Difi[9], and MinID is therefore based open standards. To log in to MinID the user must have a Norwegian social security number, PIN-code and a personal password. The first solution for logging in to MinID used PIN codes which were sent out to each user by regular postal services (snail mail). This solution is currently being phased out (but remains operative, 2012), and the new solution sends a SMS containing the PIN code to the telephone number registered together with the social security number.
One of the driving factors for this project was to increase efficiency in processing to save time and money[7], and to implement a solution such as MinID to gather all the public services and have one common solution for authentication. As it would be costly to have each governmental agency develop and operate their own solution[10]. Digital communication between the citizen

and government are cheaper than i.e. telephoning, fax, or personal meetings between citizen and public case workers. One of the motivating factors is to make as many people as possible use MinID, other related to this are these underlying motivations[7]:

- Communications with the public sector shall mainly be conducted digitally.
- All appropriate public services will be digitized.
- Digital services must be based on requirements from users, and be secure and effective.

The MinID IdMS was already implemented and had been running for several years when this PIA was conducted.

2.1.1 MinID project goals

The goal of the MinID project is to contribute to this vision by using MinID to[10, 7, 4]:
- Fulfill specification for PKI solutions as provided by the Norwegian government[8].
- Ensure access to governmental services through the use of electronic identities in a secure way.
- Establish a PKI (as defined by Difi) for using eID.
- MinID shall be secure and effective.
- Provide authorization.
- Provide eSignature.
- Provide encryption.
- Satisfy the demands for qualifying as a security level 3 solution.
- MinID must be easy to use, and shaped to fit the needs of the users.
- Customer satisfaction.
- Ensure confidentiality, availability and integrity

2.1.2 Features of the system

The system is to provide three main functionalities; authorization, digital signatures and encryption[7, 11]. Authorization is performed through the use of ID-Porten. The authentication provides access to public services such as health related services, tax and national registers[12].
Digital signatures are provided to sign documents, this is used to ensure non-repudiation and integrity. Encryption is offered through encryption of confidential documents.

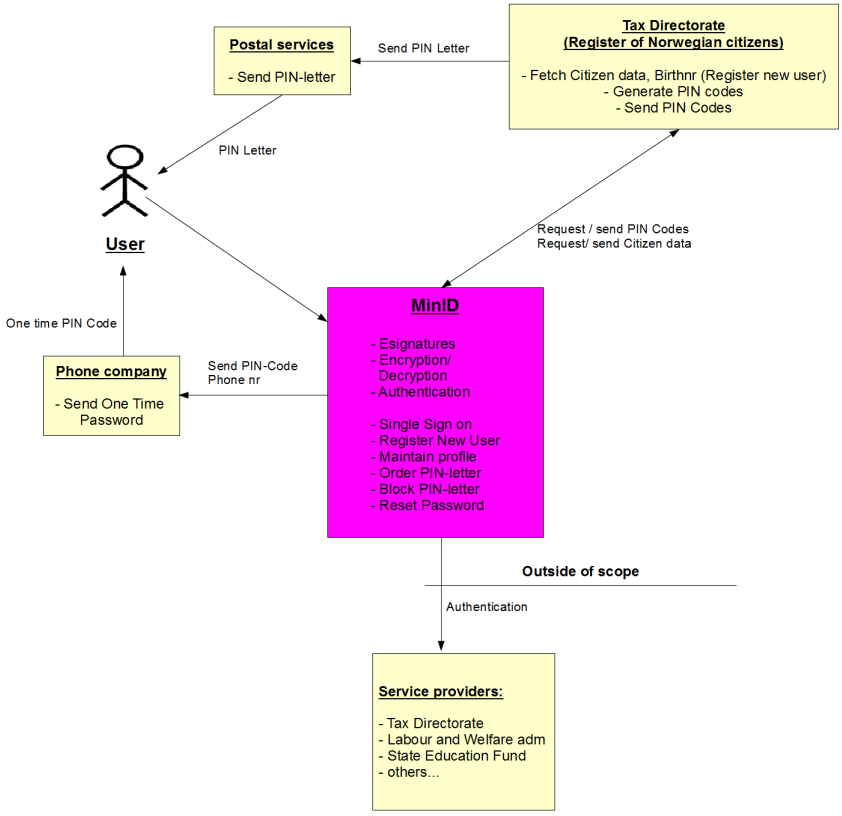


Figure 1: Features of the MinID system.

2.2 Discussion and conclusion from Initial Assessment

(Documentation for the initial assessment can be found in the appendix of this report.)
According to the Handbook, the 11 answered questions should be considered as a whole, and not individually, which means that the practitioner should conclude on the result as a whole. Out of the 11 questions from appendix 1, 7 were answered yes, 2 were answered no, and 2 questions was left inconclusive as the system documentation was not adequate to answer these two.
The results was a 64% yes from the initial assessment, which was a strong argument for performing a full scale Privacy impact assessment. The amount of people using MinID combined with the amount of personal data available through MinID, was also a strong argument for conducting a full-scale PIA. A full-scale assessment was therefore decided for.
The PIA was conducted *system specific* for MinID, with weight on the authentication and au-

thorization systems. The practitioners also retained the opportunity to adjust the PIA to fit the assignment. This was done to limit the scope and investigation of some of the bigger parts of the system.

The initial assessment of the "Privacy Law Compliance"-check yielded a yes 3 out of 3 possible, and a such a test should be part of the whole assessment. The conclusion was also that a "Data Protection Act"-compliance check is needed. Since this project is subject to Norwegian and not British law, this will be a Personal Data Act compliance check.

The conclusion was that a full scale system specific PIA is to be conducted. According to the handbook the small scale criteria questions are skipped, and the next step is criteria for Privacy Law Compliance check and after that a Data Protection Act compliance check. However, in this project the Privacy Law and the Data Protection Act Compliance check are out of scope, as this projects scope is risks posed to privacy in identity management systems, and not risks posed by being non-compliant regarding privacy laws. To answer the questions in appendix 2 of the handbook, PIA also recommends having juridical help and an intricate knowledge of the system's policy, routines, security measures and system documentation, which the practitioners do not possess.

2.3 Laws and legislations relevant for the project

MinID is a Norwegian Single sign on system, and is therefore bound by Norwegian laws and legislations. MinID also handles sensitive personal data and is therefore subject to the "Personal data act"[13] and the "Personal data regulations"[14]. The purpose of the act and regulation is to protect individuals from having their privacy violated. It should also contribute to the security of handling personal data and strengthen privacy[13].

Since Difi is a subject to the Norwegian government, there exists an act (Offentleglova)[9] that constitutes right of access to documents, journals and the likes in public administration, for which Difi must be compliant. This means that the goal of being as transparent an organization as possible is founded in the law.

Forvaltningsloven (The law of goveranace)[15] is applicable to the activities of all organs within the state or local government of Norway.

MinID is also subject to the "E-signature act"[16]. The purpose of this act is to facilitate secure and effective use of electronic signatures, and is mainly directed at certificate issuers. This is accomplished by setting requirements for the qualified certificates, the issuer of the certificates and the secure signature creation devices. The "E-governance regulation"[17] is a regulation developed to facilitate secure and effective use of electronic communication with and in the governance. It is meant to emphasize predictability and flexibility within technical solutions.

2.4 Stakeholder Analysis

The stakeholder analysis was conducted as a part of the PIA. The amount of stakeholders was reduced to 8 groups that was assessed in the project, illustrated in figure 2. The stakeholders were classified into three different classes (two of which are illustrated in the figure). The stakeholder analysis assessed each stakeholders importance, capabilities, incentives, attitude, knowledge, assets and allies. To detect risks to privacy, each stakeholders capabilities was analyzed in regard to privacy. A complete analysis of detected "malicious actions" can be found in appendix 3.

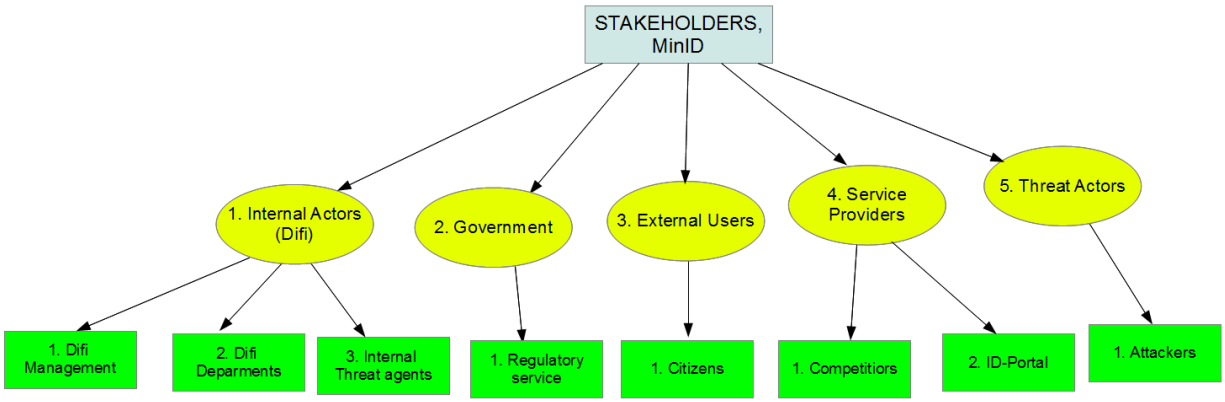


Figure 2: Categorization of stakeholders, class 1 and 2, used in this case.

3 Risk analysis

The Privacy Impact Assessment Handbook states that the main purpose of this risk analysis is to identity design issues and privacy problems with the project. And form a basis for reconsidering the design options. This focuses on the various approaches that are available to solve problems. The Handbook does not recommend any method for conducting risk analysis. This risk analysis is based on MEHARI[2], illustrated in figure 3.

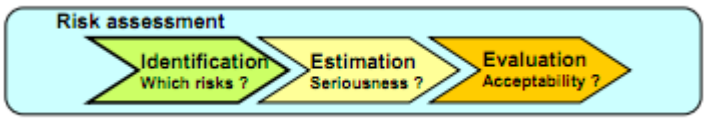


Figure 3: Summary of the MEHARI risk assessment process. *Source: CLUSIF[2]*

3.1 Risk Identification

The risk identification process was conducted as a part of the stakeholder analysis and the initial assessment conducted in PIA. Privacy is the theme of this risk analysis, and all the scenarios that have been identified to impact subscriber privacy in any way will be considered. The main assets of these scenarios is privacy related information or privacy for the citizens. These scenarios are all privacy related, the Knowledge base provided by MEHARI[2] was only used as a supplement to the identification process. The main supplement from the PIA process is the risks that were identified as a part of the initial assessment. The first 15 risk scenarios were identified in the stakeholder analysis, while the last 10 were identified used PIA:

1. Difi Management chooses to retain funding for security measures, and increase funding for other functionalities, causing a decrease in quality of security opening for external and internal attacks.
2. Difi Departments choose to access (read/write) MinID subscriber database as a part of quality improvement of services provided by i.e. customer service. Giving all internal actors access to personal data in the MinID database.
3. Difi Departments accesses high level logs (read/write) and merge them for security purposes, increasing the sensitivity of the logs.

4. The Malicious Insider reads and copies system information (including MinID database) for malicious purposes, such as espionage, data mining or selling of personal data.
5. The Malicious Insider chooses to access the MiniD database to corrupt or delete data in the MinID IdMS, i.e. to hide or corrupt data about a citizen.
6. The Malicious Insider chooses to launch a full scale attack on the system, i.e. to execute revenge on a perceived injustice.
7. Regulatory services chooses to decrease funding (or shut down) for the MinID project, resulting in less funding for security causing a decrease in quality of security.
8. User chooses to register with the MinID service, and shares his personal data with a third party creating a risk to privacy.
9. User chooses to make use of the services provided by MinID on a daily basis, causing the value of the MinID database to grow with more personal information about the user, increasing value of the logs.
10. Competitors of MinID chooses to spend money on a developing new functionality to attract users of MinID over to their own system, causing the users to share information with another third party.
11. Competitors log user information and merge these logs for security purposes, causing these logs to grow in size and increase in value.
12. The service providers in the ID-portal chooses to share personal data with the eID providers to help increase quality of service.
13. The service providers in the ID-portal uses a third party to send PIN-codes to the users for two factor authentication. Actors within the ID-portal gathers information about the users of MinID.
14. Attackers choose to attack the MinID system, either through automated or targeted attacks, to steal information. If successful the attacker can obtain sensitive information that he/she can sell for cash.
15. Attackers choose to buy personal data (i.e. from malicious insider) to exploit for further use, i.e. to reveal the location of hidden persons or blackmail.
16. (PIA) Since Difi maintains a database that stores user personal password, PIN, telephone number, social security number and behavior logs. The Malicious insider can choose to use the information kept in the logs for *surveillance, locating and tracking* individuals.
17. (PIA) MinID re-uses a multi-purpose identifier (social security number) as a part of the authentication process. The social security number can scarcely be regarded a secret, and an attacker may choose to misuse (i.e. ID-theft) the social security number of a citizen (i.e. registering MinID and steal the snail mail with PIN codes).
18. (PIA) MinID re-uses a multi-purpose identifier (social security number) as a part of the authentication process. Difi may choose to expand the use of the social security number for

quality of service or ease of access. So called "function creep".

19. (PIA) Sensitive personal data getting lost or leaked to a third party during the digitalizing of the public services the handling of information changed from mainly paper-based to digital handling.
20. (PIA) Personal data getting lost or leaked to a third party during the digitalizing of the public services, when the handling of information changes from mainly paper-based to digital handling. The MinID database also contains telephone numbers of the users. This information can be sensitive for a small percentage of the population who wants to keep their numbers confidential to avoid being found.
21. (PIA) The project handles a considerable amount of log ins and data about an individual. This data being sold to consumer marketing based on intensive profiles. It also opens for the possibility of data gathering and mining, as well as data matching. Information can also be used for surveillance, locating and tracking.
22. (PIA) The project does handle personal information concerning a large amount of individuals. This makes the system attractive to organizations and individuals trying to locate people or build marketing profiles.
23. (PIA) Increase in security measures impact a large amount of the population. The added security measure does not give privacy enough concern, and intrudes the privacy of users.
24. (PIA) The system offers functionalities that are subject to a number of laws regarding privacy. Relevant laws are not taken into account.
25. (PIA) Difi is according to Norwegian law defined as a data handler, and handles personal data and facilitates access to sensitive data about natural persons. They disregard laws and regulations, or do not realize that they are defined as a data handler.

A presentation of the above risk scenarios, assets at stake, vulnerability and threat actor is found in the table on the next page. Vulnerabilities is either violation of confidentiality (C), integrity (I) or availability (A).

Risk Overview

First 15 scenarios were detected by the Risk Analysis, and scenario 16-25 were discovered in the PIA Initial Assessment.

Risk Scenario	Asset at risk	Vulnerability (CIA)	Threat actor
1	Subscriber privacy, system security, security policies,	CIA	Internal threats External threats (Internal actors)
2	Subscriber privacy	CI	Internal threats
3	Subscriber privacy	CI	Internal threats
4	MinID database, system security, system documentation, subscriper privacy, trade secrets	C	Internal threats
5	MinID database, system security, system documentation, subscriper privacy, sensitive personal data trade secrets	I	Internal threats
6	MinID database, system security, system documentation, subscriper privacy, sensitive personal data trade secrets	CIA	Internal threats
7	Goodwill, reputation, subscriber privacy	CIA	External threats
8	Subscriber privacy	C	Internal threats External threats
9	Subscriber privacy, sensitive personal data	C	Internal threats External threats
10	Subscriber privacy, sensitive personal data	C	External threats
11	Subscriber privacy, sensitive personal data	C	External threats
12	Subscriber privacy, sensitive personal data	C	External threats Internal Threats
13	Subscriber privacy	C	External threats
14	Subscriber privacy, sensitive personal data, system documentation, system security	CIA	External threats
15	Subscriber privacy, sensitive personal data, system documentation	CI	External threats

16	Subscriber privacy	C	Internal threats
17	Subscriber privacy	CIA	Internal threats External threats
18	Subscirber privacy	C	Internal threats
19	Subscirber privacy, sensitive personal data	C	Internal threats External threats
20	Subscriber privacy, sensitive personal data	C	Internal threats External threats
21	Subscriber privacy, sensitive personal data	C	External threats
22	Subscriber privacy,	C	External threats
23	Subscriber privacy	C	Internal threats
24	Subscriber privacy, funding, goodwill, system security	CIA	Internal threats
25	Subscriber privacy, funding, goodwill, system security	CIA	Internal threats

3.2 Risk Estimation

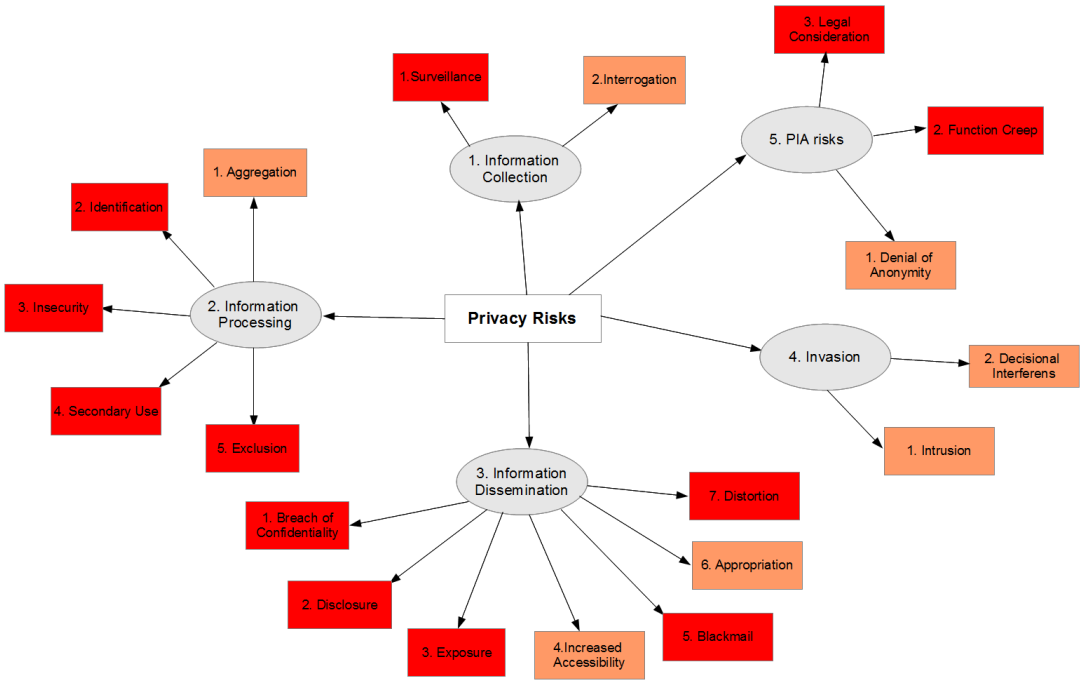


Figure 4: Graphical illustration of Risks to Privacy

The risk estimation process for this project consists of a calculation of residual likelihood of an event occurring, and the residual privacy impact for the users. The following page consists of the calculation of residual likelihood, which is intrinsic likelihood subtracted with control efficiency. This likelihood is only based on the data from the stakeholder analysis conducted as part of the PIA process. The different kinds of privacy risks are illustrated in figure 4.
An explanation for the calculations on the next page; Intrinsic likelihood = (Knowledge level + Assets Rewarded + Relationships rewarded), Control efficiency = (Assets Risked + Relationships Risked), Residual Likelihood = (Intrinsic Likelihood - Control efficiency). (For a more detailed explanation of attributes, number values, calculations and method, see Chapter 3 - Methodology in the thesis).

Residual Likelihood

Scenario nr	Actor	Knowledge level	Assets rewarded	Assets Risked	Relationship rewarded	Relationships risked	Intrisic likelihood <1>0	Control effiency <1>0	Residual Likelihood
1	Difi Management	0,6	0,3	0,3	-0,2	0,05	0,7	0,35	**0,35**
2	Difi Departments	0,6	0,25	0,15	-0,1	0,05	0,5	0,2	**0,3**
3	Difi Departments	0,6	0,2	0,15	-0,1	0,05	0,8	0,2	**0,6**
4	Internal threat agents	0,6	0,15	0,3	0,15	-0,3	0,9	0	**0,9**
5	Internal threat agents	0,6	0,15	0,3	0,05	-0,3	0,8	0	**0,8**
6	Internal threat agents	0,6	0,15	0,45	0,05	-0,3	0,8	0,15	**0,65**
7	Regulatory Services	0,4	0,15	0,35	0,05	0,3	0,6	0,65	**0,01**
8	Users	0,4	0,2	0,15	0,15	0,05	0,75	0,2	**0,55**
9	Users	0,4	0,2	0,15	0,1	0	0,7	0,15	**0,55**
10	Competitors	0,6	0,25	0,25	0	-0,05	0,85	0,2	**0,65**
11	Competitors	0,6	0,35	0,1	0	0,05	0,95	0,15	**0,8**
12	ID-portal	0,2	0,15	0,25	0	0,05	0,35	0,3	**0,05**
13	ID-portal	0,2	0,2	0,15	0,2	0,05	0,55	0,2	**0,35**
14	External Attackers	0,4	0,3	0,5	0,05	-0,4	0,75	0,1	**0,65**
15	External Attackers	0,4	0,3	0,3	0,15	-0,4	0,95	0	**0,95**
16	*See scenario 4*								
17	External Attackers	0,4	0,15	0	0	-0,1	0,55	0	**0,55**
18	Difi manag + ICT	0,6	0,25	0,15	0	0,1	0,85	0,25	**0,6**
19a	Difi manag + ICT, ID-portal	0,4	0	0,6	-0,1	0,15	0,3	0,75	**0,01**
19b	Internal threat agents	0,6	0,15	0,05	0,1	-0,1	0,85	0	**0,85**
20	*See scenario 12&13*								
21	*See scenario 4 &15*								
22	*See scenario 15*								
23	Difi manag + ICT	0,6	0,15	0,15	-0,1	0,05	0,55	0,2	**0,35**
24 & 25	Difi manag + ICT	0,6	0	0,8	-0,3	0,15	0,3	0,95	**0,01**

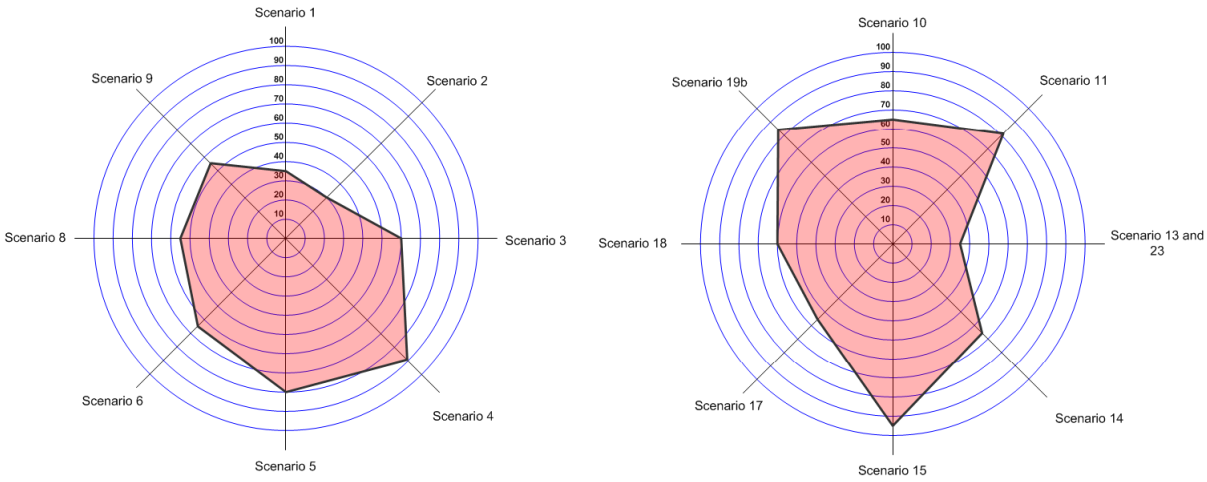


Figure 5: Graphical Illustration of likelihood

The risk scenarios that have a probability rate >0,1 are illustrated in figure 5, while the risks with probability close to zero has been left out. These risks are included in the risk classification table, where the risks are grouped together with their respective privacy risks based on the taxonomy illustrated in figure 4. The likelihood of occurance is illustrated as green - "Low" (0.01-0.25), yellow - "Medium" (0.26-0.50), orange - "High" (0.51-0.75), and red - "Very High" (0.76-0.99) (For an explanation of each privacy risk, see chapter 3 - Methodology in the thesis.)

Scenario	Likelihood of occurance	Privacy Risks (Classification)	Privacy Impact
1	Medium	Insecurity	Very High
2	Low	Increased Accessibility	High
3	High	Surveillance, Aggregation	Very High
4	Very High	Breach of Confidentiality, Disclosure	Very High
5	Very High	Distortion	Very High
6	High	Insecurity, Breach of Confidentiality	Very High
7	Low	Insecurity, Legal Consideration	Very High
8	High	Denial of Anonymity, Function Creep	Very High
9	High	Aggregation, Surveillance	High
10	High	Surveillance, Identification	Very High
11	Very High	Surveillance, Aggregation	Very High
12	Low	Denial of Anonymity, Secondary Use	Very High
13	Medium	Denial of Anonymity, Surveillance	Very High
14	High	Breach of Confidentiality	Very High
15	Very High	Breach of Confidentiality, Disclosure	Very High
17	High	Breach of Confidentiality, Blackmail	Very High
18	High	Function Creep, Secondary Use	Very High
19a	Low	Insecurity, Disclosure	Very High
19b	Very High	Insecurity, Disclosure	Very High
23	Medium	Decisional Interference, Surveillance	High
24 & 25	Low	Legal Consideration	Very High

*Scenarios 16, 20, 21 and 22 are covered by scenarios 4, 12, 13 and15.
**Scenario 19 is divided because of equal scenario with different actors.
*** Scenario 24 and 25 is combined because of their resemblance.

Figure 6: Risks to privacy and likelihood.

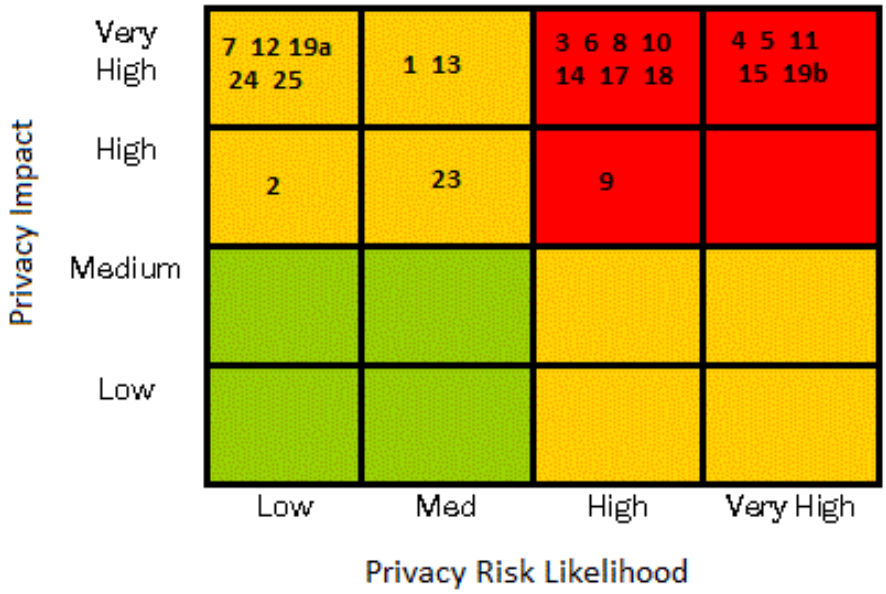


Figure 7: Privacy Risk Seriousness Matrix

4 Discussion of the Results

In this chapter the business case for MinID is discussed. The privacy issues identified in the "Risk Analysis"-chapter are discussed and the business arguments for implementing privacy intrusive technology are examined. A privacy strategy is suggested together with risk reducing measures.

4.1 Business case and Privacy intrusions

There did not exist any common solution for logging into public services electronically, and the purpose of MinID was to fill that gap. MinID was designed to be a secure and user-centric solution for logging in to public services. It is currently used (2012) to communicate an electronic identity, so that the users are authorized to use public electronic services in a secure way[10]. The system is provided by the Norwegian Agency for Public and eGovernment (Difi)[1].
The main scope is to be able to provide secure login for Norwegian citizens. The target user group for the MinID solution is everyone (above 13 years old) with a Norwegian social security number, and other users living in Norway in need of public services (users having a D-number). MinID has over 2 million users of the about 5 million people living in Norway (2012), and can be used to access more than 50 online services from various Norwegian public agencies[6]. Another group of users are the public services choosing to use MinID (ID-portal).

The system is to provide three main functionalities; authorization, digital signatures and encryption[7, 11]. Authorization is performed through the use of ID-Porten. The authentication provides access to public services such as health related services, tax and national registers[12].Digital signatures are provided to sign documents, this is used to ensure non-repudiation and integrity. Encryption is offered through encryption of confidential documents.

4.1.1 Discussion of Identified Privacy Issues

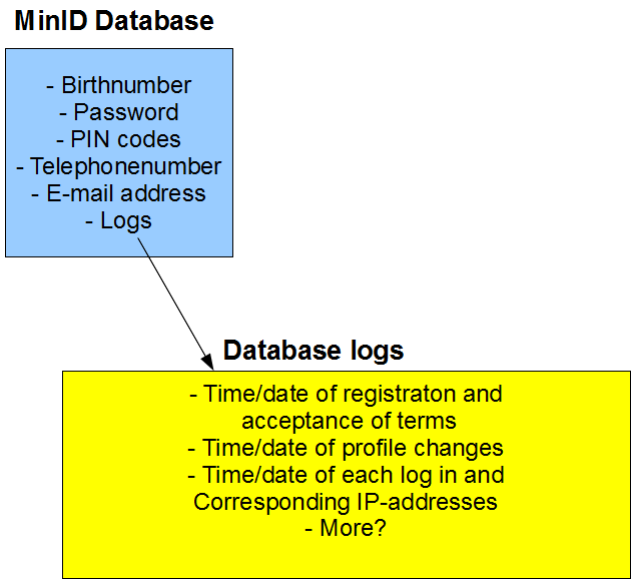


Figure 8: MinID database contents

Since the system authenticates and authorizes use of public services, it is forced to handle some sort of personal data. The personal information present in the system is illustrated in figure 8. It is unavoidable to have risks to privacy in a system that handles personal data, the identified issues and their business arguments will be examined in this section.
The system gathers information that qualifies as sensitive personal. The database logs are what makes the information in the system sensitive. These are justified through security arguments, such as to detect abuse and help prevent error. Difi should provide data to support the efficiency and necessity of these measures, to prove they are justifiable when compared to the privacy risk they create. The access to the high level logs is restricted, but having these logs present in the system creates the privacy risk of unauthorized personnel accessing them. Merging the information in these high-level logs can open for surveillance of an individual, and aggregation of data. Although implemented to help mitigate abuse and errors in the system, the high-level logs also serve to make MinID a more valuable target for external attackers.

Another issue is the extended use of the social security number as an identifier in the system. Using a identifier that includes personal data is, according to PIA not a good idea. The identifier in the MinID system is the Norwegian social security number or D-number, which can be traced back to a single individual in Norway. This means that anonymity can never be obtained when accessing services using MinID. This also raises the question if Difi needs to know the identity of every individual that accesses a service?
The original idea behind using the social security number for an identifier for MinID is unknown

to the PIA practitioners, but it is a classical case of function creep. The Norwegian social security number was originally intended for tax purposes, as a unique identifier in tax registers, but it's function has since increased, and is currently being used as an identifier in the MinID IdMS. The Norwegian SSN can scarcely be regarded a secret, as it among other things is present both the drivers license and the credit card. There has not been found any arguments for why the SSN should be used for anything else that retrieving data from the national register of people. An educated guess is that the SSN was chosen as an identifier for convenience, with no real business case to support it.

The malicious insider and the non-compliant employee is a threat in any system, and is hard to detect and avoid. In this the system, the malicious employee can sell personal data, or corrupt the data. The severity of such an action can be limited by minimizing the amount of personal data in the system.

Involvement of a third party for authentication creates risks to privacy, the PIN by telephone solution comes with some inherent risks. This solution provides the service provider with information on how often the user authenticates, and the user is identified with the service provider through his/hers registered telephone number. This solution also denies anonymity where there is no need for identification. The use of the mobile telephone does help increase security through implementing a two factor solution, but would not a RSA-chip (or something similar) served the same purpose without jeopardizing privacy.

4.1.2 Discussion of the public acceptability of the scheme

MinID is already an established actor in the ID-portal, with over 2 million users. The scheme also has two established competitors, Buypass and Commfides, which both are qualified for the Norwegian security level 4 (highest). Although the total amount of users in the ID-portal is not know to us, the amount of Norwegian citizens that can use IdMSs is just above 5 million, so 2 million is big market share. MinID qualifies for security level 3, but this does not seem to affect the public acceptability of the scheme.

4.2 Privacy Strategies, Avoidance and Reduction Measures

Based on the findings of this report and according to the handbook, the chosen strategy of Difi for MinID looks to be a "minimalist privacy strategy". This means that the most basic requirements for handling personal data is in place, such as having an understanding of the key issues when handling personal data. All the legal requirements and obligations are in place in relation to information privacy. A legal compliance and data protection check was not conducted as a part of this PIA, but based on our findings, MinID is not in violation of any laws that we are aware of.

The amount of information in the MinID database may not warrant a more comprehensive privacy strategy. The main data handled by MinID (see figure 8) is not sensitive data in itself, and consists mostly of personal data that are accessible through ordinary web searches. As far as we know, it does meet the requirements published by the Norwegian [18, 8, 4].
Although the strategy chosen may be sufficient, Difi should have considered a more comprehensive strategy. Many potential issues with their solution was detected as a part of this PIA (see chapter 3) which may have been avoided. MinID and the ID-portal impacts the Norwegian community in such a scale that "a social impacts/ public policy strategy" may be a better choice. This addresses, among other things, impacts to society; such as consequences for the citizen of he chooses not to use the solution, and job-market and industry structure impacts. It also includes privacy elements as a part of the fundamental strategy. This is not to say that Difi has not considered some of these things, but to the practitioners, it seems that Difi has a more "minimalistic" approach to privacy, than a comprehensive one.

The paramount issues in the system is discussed in section 4.1.1. Here we address risk reduction measures for each risk identified in the system. The purpose of the suggest measures is to increase customer privacy and protect privacy. Due to out lack of system specific documentation, some of these suggested measures may already be in place in the system. The four available alternatives for risk treatment are risk reduction, risk retention, risk avoidance and risk transfer. The table on the next page does not address cost of each measure, it only suggests solutions to each risk scenario.

Avoidance and Reduction Measures				
Risk Scenario	**Risk Seriousness**	**Countermeasure**	**Treatment**	**CIA**
1	High	Maintain funding for security measures	Avoidance	CIA
2	High	Implement additional access control and logging of views, such that non-repudiation can be ensured. Awareness training.	Reduction	CI
3	Very High	Implement additional access control and logging of views, such that non-repudiation and confidentiality can be ensured. Awareness training.	Reduction	CI
4	Very High	Do background checks before hiring new staff, job rotation, additional access control, protect valuable information, practice incident response	Reduction	C
5	Very High	Do background checks before hiring new staff, job rotation, additional access control, protect valuable information, practice incident response	Reduction	I
6	Very High	Do background checks before hiring new staff, job rotation, additional access control, protect valuable information, practice incident response and disaster recovery	Reduction	CIA
7	High	Perform as expected, practice incident response and disaster recovery.	Avoidance	CIA
8	Very High	Choose another identifier than the SSN to reduce privacy implications	Reduction	C
9	Very High	Choose another identifier than the SSN to reduce privacy implications	Reduction	C
10	Very High	Invest in keeping up with the competition to avoid loosing customers.	Reduction	C
11	Very High	Do nothing	Retention	C
12	High	Ensure compliance with law and legislation, and do not share personal data unless one is forced to.	Avoidance	C
13	High	Consider another solution for two factor authentication, such as RSA chip.	Avoidance	C
14	Very High	Use recommended security settings, such as firewall, IDS, Anti virus, IPS. Put focus on the human factors of information security, and prioritize awareness training.	Reduction	C
15	Very High	Implement additional access control and logging of views, such that non-repudiation and confidentiality can be ensured.	Reduction	C
17	Very High	Choose another identifier than the SSN to reduce privacy implications.	Avoidance	CIA
18	Very High	Choose another identifier than the SSN to reduce privacy implications	Avoidance	C
19a	High	Implement policies, norms and routines for data handling, and make sure they are followed. Extra protection measures valuable assets	Reduction	C
23	Very High	Do a PRA of the measure, and consider consequences for the population	Reduction	C
24 &25	High	Ensure compliance	Avoidance	CIA

Bibliography

[1] 2012. Om difi. http://www.difi.no/om-difi.

[2] 2010. Mehari 2010 - risk analysis and treatment guide. http://www.clusif.asso.fr/.

[3] 2009. *Privacy Impact Assessment Handbook Version 2.0*. Information Commissioner's Office.

[4] 2005. enorge 2009. http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eNorway_2009.pdf. (Visited Feb 2012).

[5] 2006-2007. Stortingsmelding nr 17, eit informasjonssamfunn for alle.

[6] Minid - your public id. http://minid.difi.no/minid/minid.php?lang=en. (Visited Mar. 2012).

[7] Ølnes, J. 2012. Evolution of minid and the id portal, lecture. https://wiki.uio.no/mn/ifi/AFSecurity/index.php/Main_Page. Lecture held in UiO, 250112, AF Security.

[8] 2010. Kravspesifikasjon for pki i offentlig sektor, versjon 2.0. http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/2010_Kravspek_PKI_norsk.pdf. (Visited Feb 2012).

[9] 2006. Offentlighetsloven. http://www.lovdata.no/all/hl-20060519-016.html. (Updated 2011).

[10] 2011. Minid - sikkerhet og personvern. http://www.difi.no/elektronisk-id/minid/sikkerhet-og-personvern.

[11] 2010. Kravspesifikasjon for pki. http://www.difi.no/artikkel/2010/04/kravspesifikasjon-for-pki. (Visited Feb. 2012).

[12] 2012. Virksomheter som benytter id.porten. http://www.difi.no/artikkel/2011/05/virksomheter-som-benytter-id-porten. (Visited Feb. 2012).

[13] 2000. Personal data act. http://www.lovdata.no/all/hl-20000414-031.html. (Updated 2009).

[14] 2001. Personal data regulations. http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20001215-1265.html. (Updated 2010).

[15] 1970. Forvaltningsloven (governance act). http://www.lovdata.no/all/hl-19670210-000.html. (Updated 2010).

[16] 2001. E-signature act. http://www.lovdata.no/all/hl-20010615-081.html. (Updated 2005).

[17] 2004. E-gorvenance regulations. http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20040625-0988.html. (Updated 2009).

[18] 2008. Rammeverk for autentisering og uaaviselighet i elektronisk kommunikasjon med og i offentlig sektor. http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID_rammeverk_trykk.pdf. (Visited Feb 2012).

A Appendix 1 - Initial Assessment

Initial Assessment, PIA MinID

Gaute B. Wangen

2012/06/31

Contents

1 Initial Assessment

The purpose of this section is to gather information surrounding the project, such that the screening questions, found in Appendices 1, can be answered.

1.1 Project Outline

This section consists of goals, scope and features of the the project.

1.1.1 Scope of the project

The purpose of MinID is to work as an electronic identity, so that the users are authorized to use public electronic services in a secure way [1]. The system is provided by the Norwegian Agency for Public and eGovernment (Difi) [2].
The main scope is to be able to provide secure login for Norwegian citizens who has a social security number. MinID is used by over 2 million users, and can be used to access more than 50 online services from various Norwegian public agencies [3]. MinID passes on the social security number and chosen language of the user to the service the user has chosen to log in to, the purpose of this is to work as a single sign on system.

According Difi's website [3], the system handles privacy related information, and Difi acts as a controller of the personal data handled by MinID. It holds the user's Norwegian social security number, and PIN-codes. Difi also logs information about the user's MinID use. The information kept in the user profile is mobile phone number and/or e-mail address, which is used to administrate MinID.

1.1.2 Goals and Aims of the MinID project

Difi is a governmentally owned organization, and their vision is "We develop the public sector" [2]. Difi aims to contribute to the public sector by renewing and developing it, and strengthen cooperation between vendors and offer joint solutions. The goal of this project is to contribute to this vision by using MinID to [1, 4, 5]:
- Fulfill specification for PKI solutions as provided by the Norwegian government [6].
- Ensure access to governmental services through the use of electronic identities in a secure way.
- Establish a PKI (as defined by Difi) for using eID.

- MinID shall be secure and effective.
- Provide authorization.
- Provide eSignature.
- Provide encryption.
- Satisfy the demands for qualifying as a security level 3 solution.
- MinID must be easy to use, and shaped to fit the needs of the users.
- Customer satisfaction.
- Ensure confidentiality, availability and integrity

1.1.3 Features of the system

The system is to provide three main functionalities; authorization, digital signatures and encryption [4, 7]. Authorization is performed through the use of ID-Porten. The authentication provides access to public services such as health related services, tax and national registers [8].
Digital signatures are provided to sign documents, this is used to ensure non-repudiation and integrity. Encryption is offered through encryption of confidential documents.

1.1.4 Documentation

Although we were unable to find any documentation on the inner workings of MinID, one of their objectives is to base the design on open standards [9]. A summary of the documentation available through their website and other sources is available in the case developed as a part of this project. The project goals and what services they provide are well documented, and openly available.

1.2 Stakeholder analysis

This analysis is to contain a list of groups or organizations who may have an interest in, a role to play in delivering, or be affected by the project.

CATEGORY 1 NAME	CATEGORY 2 NAME	CATEGORY 3 NAME	PURPOSE
Internal actors			
	Human threat agents	Malicious insider	
		Cleaning staff	
		Physical security responsible	
	Difi management	CEO	
		Board of directors	
		IT security responsible	
		Policy Creators	
		Routine makers	
		Supervisors	
	Difi Operators	Network operators	
		Telecommunication Operators	
		Misc operators	
	Difi creative side	Developers	
		Programmers	
		Testers	
		Project developers	
	DIFI miscellaneous	General Employee	
		Lawyers, and/or other legal contributors	
		Service/support employees	
Governmental Prerequisite	Datatilsynet (http://www.datatilsynet.no/Om-Datatilsynet/Oppgaver/)	Privacy auditors	-Make sure laws og legistlations are followed - detect privacy risks - Ensure compliance
		Privacy advisors	- Counselling on how to avoid/mitigate privacy risks etc. - Help develope norms
	Complaint handlers (http://www.personvernnemnda.no/om.htm)	Personvernnemda	Handle complaints regarding to decisions done by datatilsynet and privacy laws.
	Non-specific Norwegian Government	Policy makers	
		Law and legislation makers	
	Financial	Performance indicators / Funding responsible	
	Ministry of Government Administration, Reform and Church Affairs		

	(FAD)		
Commercial (users)			
	Citizens	PIN users (Norwegian)	
		D-number users (Non-norwegian)	
	Municipalities		
	Other governmentally owned users		
Service Providers			
	ID-porten partners	Buypass	
		Commfides	
	Software suppliers	OASIS (SSO system)	
		OpenAM (Access management, ForgeRock AS)	
	Hardware suppliers	Telephone company	
		(Posten – Shipping of Pin codes)	
	Project partners	Brønnøysund registrenene	
		Health services	
		Nav	
		Lånekassen	
		Others.	
External threat actors			
	Human attackers	Hacker/Crackers	
		Computer criminals	
		Terrorist	
		Industrial spies	
	Non-Human attackers	Virus	
		Worms	

1.3 Environmental scan

The purpose of this section is to find out what else is out there. The search did not find any prior PIAs on similar IdMS. However many prior PIA reports on information systems was found, although not entirely related, they reveal most of how their PIA were conducted and give some good pointers on what the report should look like. A summary of documentation, fact sheets, white papers and other sources are found in the case study.

2 PIA screening process

This chapter contains the PIA screening process. This process is used to determine what kind PIA should be conducted. As described in the PIA Handbook v2.0, we will start with the 11 questions about key project characteristics, labeled as step 1-Criteria for full-scale PIA.

2.1 Criteria for full-scale PIA

According to the handbook, these 11 questions represent characteristics of projects which have significant risk factors concerning privacy. To able to answer these questions as correctly as possible, we have made the assumption that we are in the implementation/testing phase of the project. Since MinID is part of the digitalization of Norway, the questions regarding change are answered with the transition from paper to digital public services as a basis.

1. **Technology**
   Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?
   Yes. The project applies a personal password and a one time PIN-code sent to the user's mobile telephone, or a personal password and a one time PIN-code from a personal PIN-letter received through postal services. Difi state on their website that they the system handles privacy related information [3]. Difi maintains a database that stores the user's personal password and social security number which is sent to them from Skatteetaten.
   These technologies by themselves have little potential for privacy intrusion, but Difi also logs user behavior when using MinID [1]. It is stated that these logs are used to help prevent abuse. Difi's web pages does not specify what type of behavioral information that is being logged. These type of logs have substantial potential for privacy intrusion.
2. **Identity**
   Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?
   Yes, the project uses MinID which is a multi purpose identifier. MinID can be used for authentication, digital signatures and encryption [4]. MinID is used to sign into an identity management system that can be used to access electronic services. The system uses the individual social security number together with MinID as an identifier.
3. **Identity**
   Might the project have the effect of denying anonymity and pseudonymity, or converting transac-

tions that could previously be conducted anonymously or pseudonymously into identified transactions?
Given the vast amount of services offered in ID-porten, it is likely that the project might have had that effect on anonymity and pseudonymity for some services. However, the system has already been implemented and has been running for a couple of years. It is difficult to know the state of previous services before ID-porten was implemented. We were unable to find any such services in our searches. Due to the amount of services available through MinID, this is likely to have happenend. But we are unable to provide a conclusive answer.

4. **Multiple organizations**
Does the project involve multiple organizations, whether they are government agencies (eg in 'joined-up government' initiatives) or private sector organizations (eg as outsourced service 'providers or as 'business partners')?
Yes, the project provides access to multiple government agencies, and the services offered by these. The companies Buypass [10] and Commfides [11] also provide access to the same services as MinID. While MinID mainly provides services to governmental services, Buypass and Commfides also deliver services to the private sector. Commfides is privately owned, while Buypass is owned by EDB Ergo Group and Norsk Tipping.

5. **Data**
Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals?
Yes, this project was a part of the transition from paper-based to electronic-based public services. The handling of data is therefore changed. MinID handles the user's social security number, personal password, mobile telephone number and logs on user behavior. According to the definition provided by the Personal data act [12] ğ2.1, personal data can also be information that can be linked to an individual, and the handling occurring with MinID is interperated to be inside of this scope (a social security number can be linked to an individual). MinID is also used to access services which contain and handle sensitive personal data, and are according to the law, within the definition (provided in ğ2.2 of the Personal data act [12]) of "processing of personal data". And according to ğ3.a, they are then subject to the Personal data act.

6. **Data**
Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?
Yes. According to their web page [3] and Norwegian law they handle personal data (see answered question 5). The system facilitates access to i.e. welfare administration and health care. What "a considerable amount of personal data about each individual" is hard to define. Difi has, through the implementation of MinID, changed the handling of personal data about each individual in the database.

7. **Data**
Does the project involve new or significantly changed handling of personal data about a large number of individuals?

Yes. Last year, MinID grew to over 2 million Norwegian users [13].

8. **Data**
   Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?
   It is very likely, though currently unconfirmed, that the user logs in Difi's systems are cross-referenced to detect abuse. Examples is cross-referencing IP-addresses from previous log ins, and merging the logs. But as this currently is unconfirmed, the answer to this is inconclusive.

9. **Exemptions and Exceptions**
   Does the project relate to data processing which is in any way exempt from legislative privacy protections?
   No, we are not currently aware of such exemptions or exceptions.

10. **Exemptions and Exceptions**
    Does the project's justification include significant contributions to public security measures?
    Yes, MinID is a public solution available for everyone with a Norwegian social security number or a D-number. One of the visions of the Norwegian government is to digitize as much of the public services as possible, and to make the services available for every Norwegian citizen. The security measures in the MinID solution therefore adds to the overall security of Norwegian citizens.

11. **Exemptions and Exceptions**
    Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?
    No, we are currently not aware of any services available through MinID that are not subject to Norwegian privacy laws and regulations.

2.2 Discussion and conclusion on initial assessment

According to the Handbook, the 11 answered questions should be considered as a whole, and not individually. Out of the 11 questions from appendix 1, 7 were answered yes, 2 were answered no, and 2 question was beyond our current ability to answer. We have a 64% yes from the initial assessment, which is a strong argument for performing a full scale Privacy impact assessment. The amount of people using MinID combined with the amount of personal data available through MinID, is also a strong argument for conducting a full-scale PIA.
The PIA will be conducted *system specific* for MinID, we also retain the opportunity to adjust the PIA to fit our assignment. This is to limit the investigation of some of the bigger parts of the system.

The conclusion is that a full scale system specific PIA is to be conducted. According to the handbook the small scale criteria questions are skipped, and the next step is criteria for privacy law compliance check.

2.3 Criteria for privacy law compliance checks

The purpose of this section is to determine if a Privacy Law Compliance check should be conducted. The project warrants such a check if one of the three following questions are answered yes.

1. *Does the project involve any activities (including any data handling), that are subject to privacy or related provisions of any statute or other forms of regulation, other than the Data Protection Act?*
   Yes, besides the Data Protection Act [12], the project is subject to the E-signature act [14], as MinID is used to provide electronic signatures. Forvaltningsloven (Governance Act) [15] is applicable to the activities of all organs within the state or local government of Norway. Universal laws for which MinID is subject is the human rights act [16], article 3, 12, 21, 22.
2. *Does the project involve any activities (including any data handling) that are subject to common law constraints relevant to privacy?*
   Yes, the system facilitates access to sensitive personal information. Difi is defined by law [12] as a data handler, and are therefore subject to laws and regulations that are imposed on data handlers.
3. *Does the project involve any activities (including any data handling) that are subject to less formal good practice requirements relevant to privacy?*
   Yes. In a document published by Difi in 2010 [17], it specifically mentions that best practices developed in Norway are founded in ISO/IEC 27001:2006 and SS-ISO/IEC 27002:2005. Although it does not specify that these standards have been used in the development of MinID, it is likely that they have been since it is a from a framework for authentication and non repudiation in electronic communication in the public sector. We make the assumption that they have to be able to answer the question.

The questions were answered three out of three yes. This means that a Privacy Law Compliance check *will be conducted*.

2.4 Criteria for Data Protection Act compliance checks

This criteria is used to determine if a Data Protection Act compliance check is needed. This check consists only of one question. This question in its original form contains definitions provided by UK law, this have been altered to fit Norwegian law.

1. *Does the project involve the handling of any data that is personal data, as that term is used in the Personal Data Act [12]?*
   1) Personal data: any information and assessments that may be linked to a natural person.

The definition of sensitive personal data provided by Norwegian law [12], ğ2.8: " ... information relating to
a) racial or ethic origin, or political opinions, philosophical or religious beliefs,
b) the fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act,
c) health,
d) sex life,
e) trade-union membership.'
"

Yes, MinID handles personal data. It also facilitates access to information that is regarded as sensitive personal data.

The conclusion is that a Data Protection Act compliance check is needed. Since this project is subject to Norwegian and not British law, this will be a Personal Data Act compliance check.

3 Initial Assessment of Privacy Risk

We found that a full-scale PIA is warranted, together with a Privacy law compliance check and a Data Protection Act compliance check. This initial assessment of potential privacy risks in the system is based on the previous findings in this document. This is merely a first attempt at identifying privacy risks, and has only been considered from the perspective of the external consultant. Based on the PIA handbook, these are the initial risks that have been found:

- Difi maintains a database that stores user personal password, PIN, telephone number, social security number and behavior logs. These technologies have a potential for privacy intrusions.
- The project uses a multi-purpose identifier, that according to the handbook, come with a considerable amount of privacy risks. It also re-uses social security numbers as a part of the authentication process.
- Changed handling of personal information. In the digitalizing of the public services the handling of information changed from mainly paper-based to digital. According to the handbook this presents a risk to privacy. Difi's database contain Norwegian social security numbers which are a central piece of information for criminals wanting to commit identity theft in Norway.
- The project involves changed handling of personal data that is in particular concern to individuals. MinID handles or provides access to financial information regarding individuals, health information, etc... The MinID database also contains telephone numbers of the users. This information can be sensitive for a small percentage of the population who wants to keep their numbers confidential to avoid being found.
- The project handles a considerable amount of log ins and data about an individual. Such information poses risks to privacy, because it is especially attractive to consumer marketing based on intensive profiles. Information can also be used to map user behavior.
- The project does handle a personal information concerning a large amount of individuals. This makes the system attractive to organizations and individuals trying to locate people or build marketing profiles.
- The project comes with an increase in security measures that impact a large amount of the population. According to the handbook, measures that impact a large percentage of the population tend to have a substantial impact on privacy. And there has been tendencies not to give privacy enough concern, creating a tension between with privacy risks.

- The system offers functionalities that are subject to a number of laws regarding privacy.
- Difi is according to Norwegian law defined as a data handler, and handles personal data and facilitates access to sensitive data about natural persons. This role comes with an inherent risk to privacy.
- (Probable cross referencing, interlinking and matching of personal data. Difi uses logging of user behavior to detect abuse. These logs can i.e. be abused for profiling of the user.)

Bibliography

[1] 2011. Minid - sikkerhet og personvern. http://www.difi.no/elektronisk-id/minid/sikkerhet-og-personvern.

[2] 2012. Om difi. http://www.difi.no/om-difi.

[3] Minid - your public id. http://minid.difi.no/minid/minid.php?lang=en. (Visited Mar. 2012).

[4] Ølnes, J. 2012. Evolution of minid and the id portal, lecture. https://wiki.uio.no/mn/ifi/AFSecurity/index.php/Main_Page. Lecture held in UiO, 250112, AF Security.

[5] 2005. enorge 2009. http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eNorway_2009.pdf. (Visited Feb 2012).

[6] 2010. Kravspesifikasjon for pki i offentlig sektor, versjon 2.0. http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/2010_Kravspek_PKI_norsk.pdf. (Visited Feb 2012).

[7] 2010. Kravspesifikasjon for pki. http://www.difi.no/artikkel/2010/04/kravspesifikasjon-for-pki. (Visited Feb. 2012).

[8] 2012. Virksomheter som benytter id.porten. http://www.difi.no/artikkel/2011/05/virksomheter-som-benytter-id-porten. (Visited Feb. 2012).

[9] 2009. Difi - utvikling gjennom samarbeid. http://www.difi.no/filearchive/brosjyre-om-difi-pdf-.pdf. (Visited Mar. 2012).

[10] Buypass - om buypass. http://www.buypass.no/om-buypass. (Visited March 2012).

[11] Commfides. https://www.commfides.com/Om-Commfides/Om-Commfides.html. (Visited March. 2012).

[12] 2000. Personal data act. http://www.lovdata.no/all/hl-20000414-031.html. (Updated 2009).

[13] 2010. To millioner kan legge bort pin-kodene. http://www.difi.no/artikkel/2010/04/to-millioner-kan-legge-bort-pin-kodene. (Visited Feb. 2012).

[14] 2001. E-signature act. http://www.lovdata.no/all/hl-20010615-081.html. (Updated 2005).

[15] 1970. Forvaltningsloven (governance act). http://www.lovdata.no/all/hl-19670210-000.html#map0. (Updated 2010).

[16] 1948. The universal declarations of human rights. http://www.un.org/en/documents/udhr/.

[17] 2010. Risikovurdering - en veiledning til rammeverket for autnetisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor. http://www.difi.no/filearchive/rapport-veiledning-til-rammverket-versjon-0-1.pdf.

B Appendix 2 - Project Background Paper

Project background

Gaute B. Wangen

2012/06/31

1 Project Outline

This document is created as a deliverable in the Privacy Impact Assessment of MinID. It contains an extended project outline, based on the work conducted in the initial assessment.

1.1 Context description and motivation

In 2005, the Norwegian government published a document called "eNorway 2009" [1], which together with "‘Stortingsmeldingen nr 17" [2] form the basis for the governments goal of digitalizing the public services in Norway. One of the main purposes of this was an efficiency process, where moving from paper based services to digital public services was essential.
Difi, which is the Agency for Public Management and eGovernment in Norway, has a mandate to establish a common infrastructure for using electronic identities i the public sector [3]. Requirements for a Public key infrastructure(PKI) [4] in Norway was published in 2005 (later updated in 2010), which forms the foundation for the common infrastructure in Norway. Difi has created the solution MinID, which is a personal electronic identity. MinID can be used to log in to a single access point, which facilitates access to a wide range of available public services [5]. MinID is currently one of three available solutions for logging in to the "ID-portal" which facilitates access to available public services.
Transparency is important to Difi [6], and MinID is therefore based open standards. To log in to MinID the user must have a Norwegian social security number, PIN code and a personal password. The first solution for logging in to MinID, used PIN codes which were sent out to each user by regular mail services. This solution is currently being phased out (but remains operative), and the new solution sends a SMS containing the PIN code to the telephone number registered together with the social security number.
One of the driving factors for this project was to increase efficiency in processing to save time and money [3]. Digital communication between the citizen and government are cheaper than i.e. telephoning, fax, or personal meetings between citizen and public case workers. Another related factor is to make as many people as possible use MinID. Related to this are these underlying motivations [3]:

- Communications with the public sector shall mainly be conducted digitally.
- All appropriate public services will be digitized.
- Digital services must be based on requirements from users, and be secure and effective.

Another motivating factor for implementing a solution such as MinID, is to gather all the public services and have one common solution for authentication. It would be costly to have each governmental agency develop and operate their own solution [7].

The PIA project is conducted on an already implemented solution, and is conducted as a part of the project called PETweb II.

1.2 Business Rationale

There did not exist any common solution for logging into public services electronically, and the purpose of MinID was to fill that gap. And be a secure and user-centric solution for logging in to public services. It is currently used to communicate an electronic identity, so that the users are authorized to use public electronic services in a secure way [7]. The system is provided by the Norwegian Agency for Public and eGovernment (Difi) [5].
The main scope is to be able to provide secure login for Norwegian citizens. The target user group for the MinID solution is everyone (above 13 years old) with a Norwegian social security number, and other users living in Norway in need of public services (users having a D-number). MinID has over 2 million users of the about 5 million people living in Norway (2012), and can be used to access more than 50 online services from various Norwegian public agencies [8]. Another group of users are the public services choosing to use MinID (ID-portal).

The system is to provide three main functionalities; authorization, digital signatures and encryption [3,9]. Authorization is performed through the use of ID-Porten. The authentication provides access to public services such as health related services, tax and national registers [10].
Digital signatures are provided to sign documents, this is used to ensure non-repudiation and integrity. Encryption is offered through encryption of confidential documents.

1.2.1 Business objectives

Difi is a governmentally owned organization, and their vision is "We develop the public sector" [5]. Difi aims to contribute to the public sector by renewing and developing it, and strengthen cooperation between vendors and offer joint solutions. The goal of this project is to contribute to this vision by using MinID to [1,3,7]:
- Ensure confidentiality, availability, integrity and non-repudiation for all services.
- Provide common solutions for authorization, eSignature and encryption in the public sector.
- Establish a PKI for using eID according to public requirements for PKI solutions [4].
- Ensure access to governmental services through the use of electronic identities in a secure and effective way.
- Satisfy the demands for qualifying as a security level 3 solution.
- MinID must be user centric and available to as many people as possible.

- Obtain as many users as possible.

1.3 Personal information flows

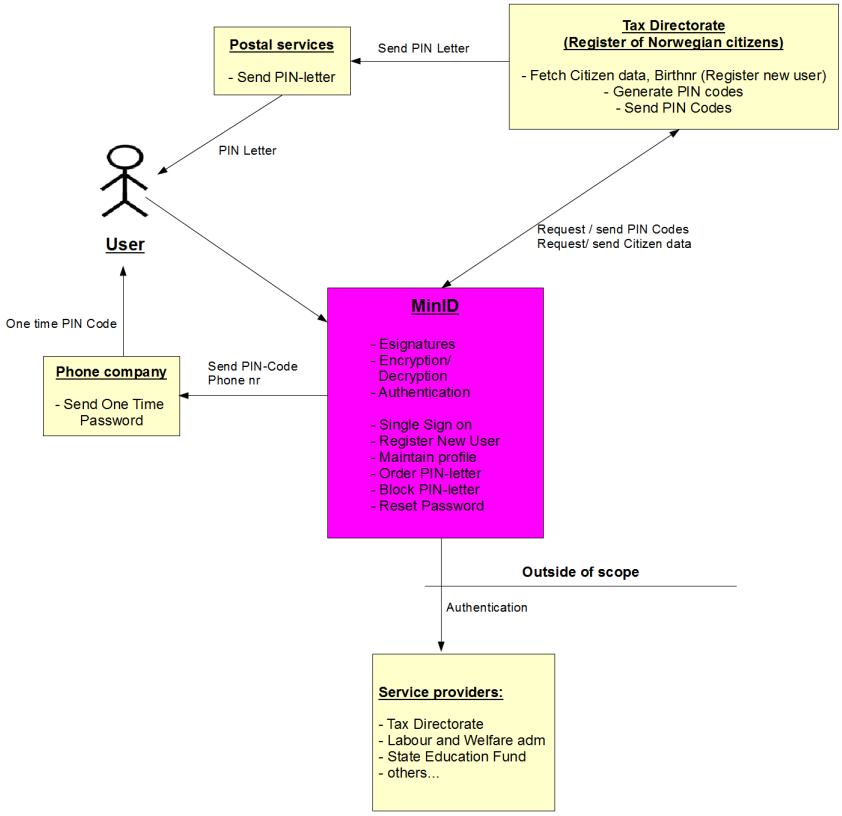


Figure 1: MinID IDMS illustrated as a SSO. The only personal data handled is that which is gathered and present in MinID systems. This figure also illustrates the provided services and connections that MinID makes (that we are aware of).

MinID has a database that consists of a social security number/birthnumber (our guess is that this is also the primary key for the database entry), password (possibly hashed), pin codes, telephone number, e-mail and log about usage. This is illustrated in figure 2.

Authentication is one the most common applications of MinID. The information flow for authenticating using MinID is illustrated in figure 3. The personal information that is being provided

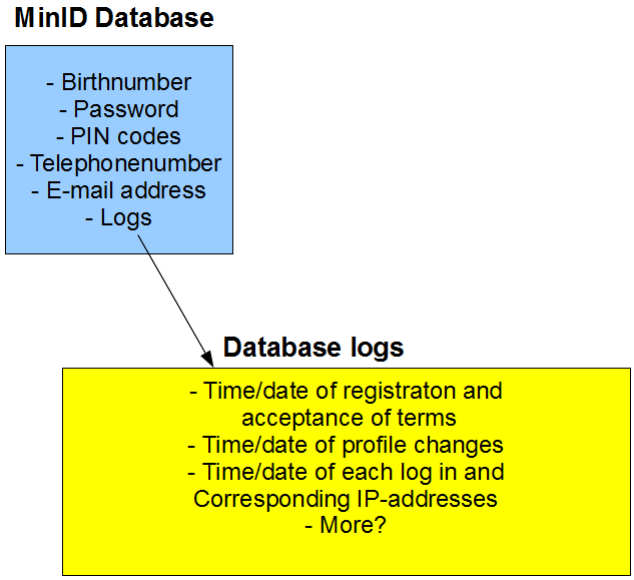


Figure 2: Illustration of personal information stored about each user in the MinID database.

by the user is his social security number (birthnumber) and password. When these two pieces of information have been provided, the account in the database is found, presumably by using the birthnumber. The one time PIN-code is sent to the registered mobile telephone, using SMS. The user is prompted for the PIN code, and can successfully authenticate when he types in the code he received via his mobile phone. MinID then passes on the user's birthnumber and chosen language (Norwegian or English) to the chosen service provider.

1.4 Potential Privacy Risks discovered in the Initial assessment

An initial evaluation of the risks that were discovered during the initial assessment, using the risk factors described in the Handbook:

- Difi maintains a database that stores user personal password, PIN, telephone number, social security number and behavior logs. These technologies have a potential for privacy intrusions, such as data matching and data mining. Routines for accessing and altering information is in place, and options for unregistering information is present in the system. Future consequences of unregistering for this service is that the user will have use telephone, e-mail, mail or other services to interact with the public services. The information kept in the logs (see figure 2) can be used for locating and tracking individuals. The database records IP-addresses which disclose the time and the geographical location of log ins, which can be used for both surveillance, locating and tracking.
- The project uses a multi-purpose identifier, that according to the handbook, come with a

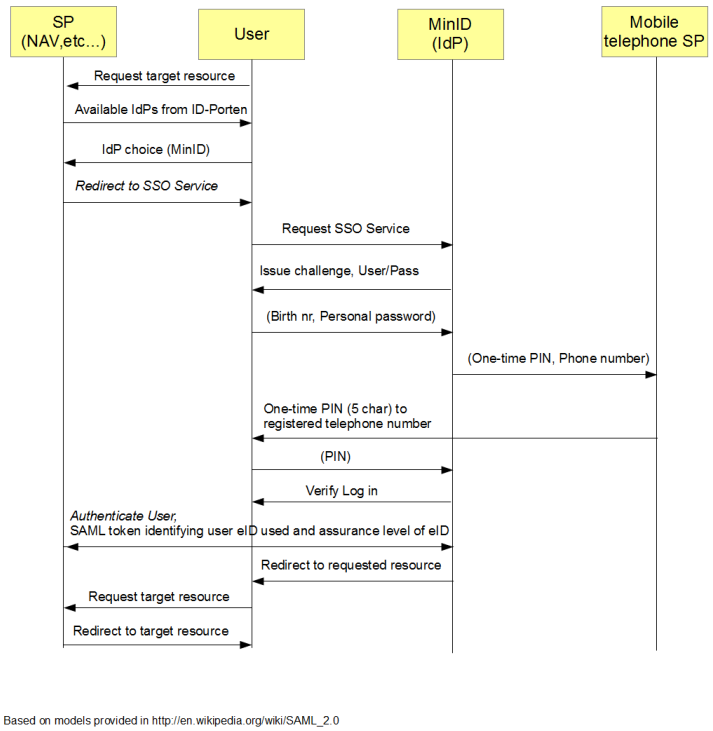


Figure 3: Information flow for authentication with MinID.

considerable amount of privacy risks. It also re-uses social security numbers as a part of the authentication process. The use of social security numbers as part of the authentication can be problematic, as it is an identifier that directly discloses personal data. One may argue that the social security number has also been victim for so-called "function creep", where the use of the social security number has grown and expanded beyond what was the original context and scope.

- Changed handling of personal information. In the digitalizing of the public services the handling of information changed from mainly paper-based to digital handling. According to the handbook this presents a risk to privacy. Difi's database contain Norwegian social security numbers which are a central piece of information for criminals wanting to commit identity theft in Norway.
- The project involves changed handling of personal data that is in particular concern to individuals. MinID handles or provides access to financial information regarding individuals, health information, etc... The MinID database also contains telephone numbers of the users. This information can be sensitive for a small percentage of the population who wants to keep their numbers confidential to avoid being found.
- The project handles a considerable amount of log ins and data about an individual. Such

B Appendix - Risk IT report

Risk IT Report

Gaute B. Wangen

2012/06/31

Abstract

This Risk IT report was conducted as a deliverable of the master's thesis "Risk Analysis for Privacy and Identity Management", which was carried out at Gjøvik University College spring semester 2012. The framework that was followed in this report was "The Risk IT Framework" [1] from 2009 provided by ISACA. The identity management system (IdMS) assessed in this report was "MinID", which was provided by the Norwegian Agency for Public Management and eGovernment (Difi).

The purpose of this report is to contribute to the thesis as a foundation for comparison between two risk analysis standards. The scope of this assessment is mainly the risk analysis part of the framework. A data flow diagram analysis was used as risk identification technique.

Contents

1 Introduction and Risk Universe

The target of this Risk IT report is the MinID identity management system (IdMS) provided by the Norwegian Agency for Public Management and eGovernment (Difi). The goal of this process is to conduct a risk analysis of how the system handles privacy related information and to discover potential risks to privacy. The framework that was followed in this report was "The Risk IT Framework" [2] and "The Risk IT Practitioner Guide" [1] from 2009 provided by ISACA. The scope of this report is to conduct a risk identification and analysis. The rest of the assessment process, such as countermeasures, risk management strategies, and similar activities are outside of the scope of this report.

MinID is a part of the "ID-portal" (ID-porten) which can be logged into using MinID, Buypass and Commfides. All three can be used to access public services like tax, health services and many others. In April 2010 the number of registered Norwegian citizens using MinID increased to over 2 million users [3].

1.1 Overview of Difi and MinID

Difi is a governmentally owned organization, and their vision is "We develop the public sector" [4]. Difi aims to contribute to the public sector by renewing and developing it, and strengthen cooperation between vendors and offer joint solutions.
Difi is divided into ten units [5], whereas management is formed out of three units, CEO, assistant director and the communications unit (KEN). The seven sub-departments have different responsibilities within the organization.
Their goal concerning electronic identities is to establish a joint infrastructure for use of electronic identities in governmental sectors [6]. To achieve this objective they have developed the solution known as MinID. The main objective of MinID is to ensure access to governmental services through the use of electronic identities in a secure way [7]. One of the main reasons for implementing ID-porten and MinID is the amount of time and money that can be saved through digitalization of the public services.

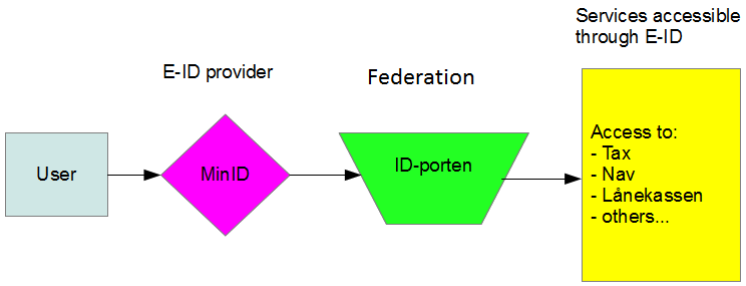


Figure 1: Graphical Illustration of the ID-portal

Figure 1 shows a top-down view of the user authenticating through the ID-portal to access public services. To log in using MinID, the user applies his Norwegian personal identification number (consists of 11 numbers) or D-number (temporary number given to foreign citizens that pay taxes to Norway) [8], a password and a PIN code. The PIN code is either found on piece of paper containing several codes delivered by mail, or it can be sent to the user's mobile telephone if he/she has registered the telephone number. The latter is becoming the more common solution [4], as paper is an old-fashioned solution. Other goals of for Difi and MinID are [6]:

- That the public sector will use Difi's knowledge, means and tools, something which is achievable only through cooperation and dialog.
- Good cooperation with the rest of the management is the most important prerequisite for Difi's success.
- Difi has a special responsibility for the renewal and development of public sector in the areas of ICT, procurement, communication, organization, instruments and training.
- Transactions between citizens and the government should mainly be digitalized.
- Digital solutions shall be offered for all suitable governmental services.
- Digital services shall be shaped by the user's need and be secure and effective.
- Handle foreign logins.
- MinID is to be based on open source solutions.
- Be transparent according to laws and legislation.

1.2 Scoping IT Risk Management

The boundaries of this risk assessment will be the IdMS provided by Difi. MinID is defined as a standalone system, and is not responsible for information accessed using MinID [9]. The risk assessment process will not go beyond risk identification and risk analysis, countermeasures and

risk management strategies will not be discussed in this report.
Only the IT-related parts of the system will be considered. The main focus of this assessment will be the parts of the system that handle personal data. The authentication feature is the main functionality of MinID, and this is also where most of the privacy related information is being handled. The encryption/decryption and digital signatures features of the system will not be considered as a part of this assessment.
Since the main topic of this report is privacy, the risk management process will only include the system parts that handle personal data. The main scope will therefore be the authentication feature, personal data storage and usage.

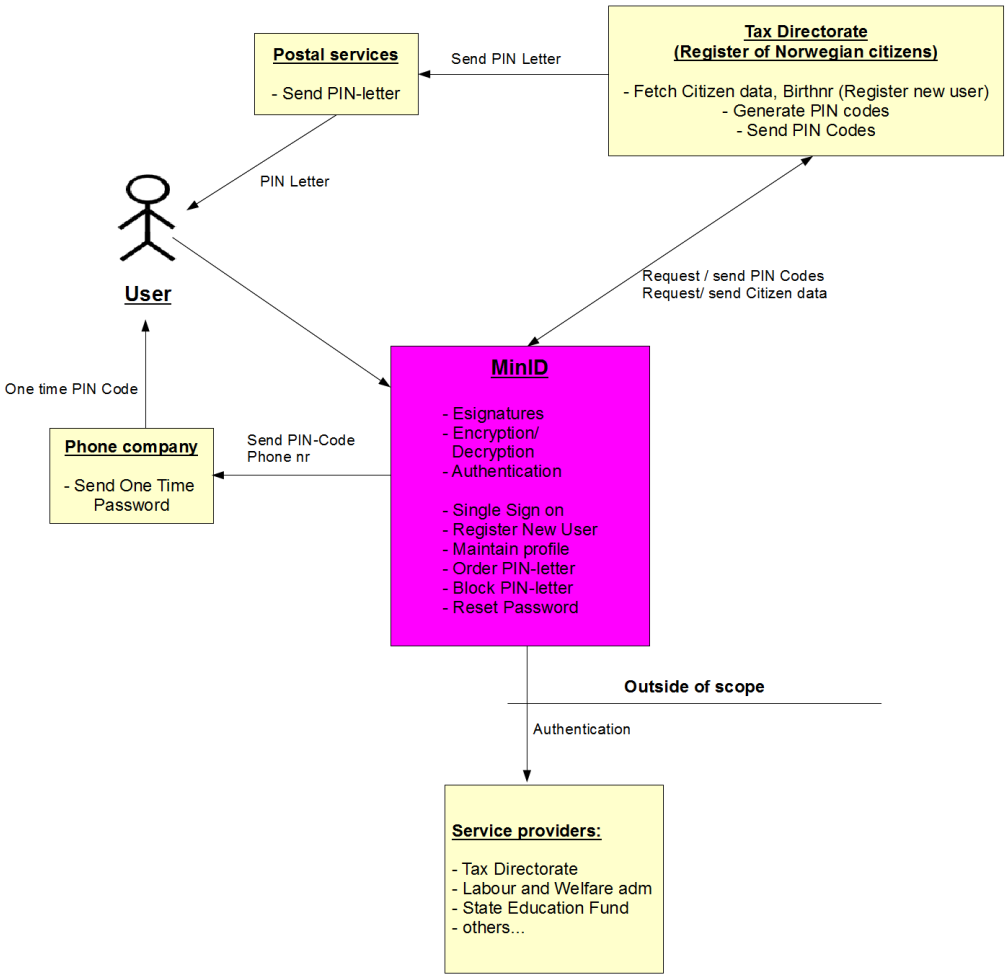


Figure 2: The MinID system

Figure 2 shows the MinID system, and it's connections to third parties through offered services. This figure also helps illustrates the scope of this report. The purple rectangle in the middle of the figure represents the main scope of this assessment, but the connections from the system processes to third parties will also be assessed.

1.3 Business Goals

Difi developed the MinID solution and operates the IdMS on a day to day basis. Difi is funded by the government, and the assumption is made that it is a non-profit organization. Since the solution already has been running a while, some of these goals are partly accomplished. Their business goals are the following:

- Have as many users as possible using MinID.
- Keep MinID up, running and available 99.9% of the time.
- Maintain integrity of the MinID service.
- Maintain confidentiality of the MinID service.
- Maintain customer satisfaction to prevent them from choosing other eID providers.
- Contributions to the Public Services (ease of access, digitalization of services, knowledge).
- Keep the solution compliant.
- Avoid security incidents.
- Maintain funding for the solution.

1.4 IT applications and infrastructure

One of the goals of Difi is to be transparent according to laws and legislation, and is because of this based on open source products. According to Østvold and Difi's website [10, 11], the design of ID-porten is based on the OASIS SAML 2.0 standard for web services [12], OpenAM from ForgeRock AS [13], and the OpenDS Directory Sever [14]. OASIS SAML 2.0 is an open standard for exchanging authentication and authorization data between security domains.
The system was modeled into two data flow diagrams as a part of the privacy risk identification process. These two diagrams are detailed descriptions of the system and can be seen in figure 7 and 8.

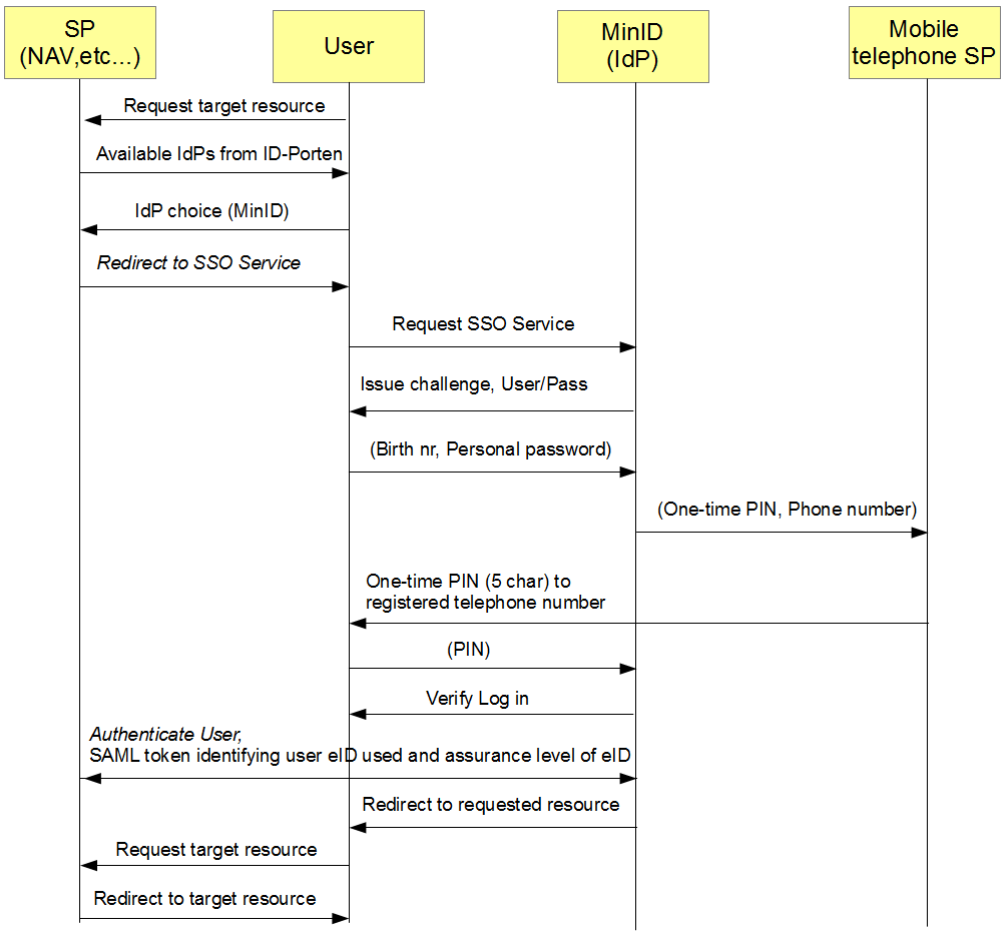


Figure 3: MinID authentication

Figure 3 shows the parts involved in an authentication using MinID, and how the flow of information unfolds between the different actors. This model is based on the SAML 2.0 model, and modified to fit the two factor authentication model of MinID, using a one time PIN sent to the mobile telephone. The user logs in with his social security number (SSN) and his private password, and after having done this receives a one time PIN-number to his registered mobile telephone number.

The data being about each user in the MinID database is illustrated in figure 4. Which holds all the personal data (that is known) in the system. The database entry for each user is created when the user registers for the service. The MinID database uses the SSN, of the user registering, to retrieve user data from the Tax Directorate's register of Norwegian citizens. The user has some options in the MinID system, such as authentication, maintaining personal data, choosing either PIN-letter or mobile telephone for authentication, unregistering and others which will be

examined in detail in chapter 2.

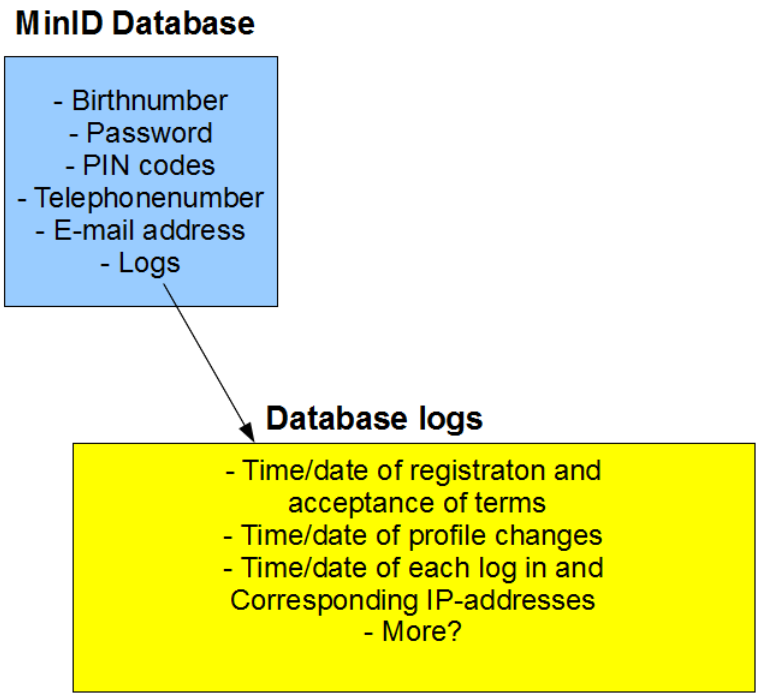


Figure 4: An illustration of the personal information stored in the MinID database.

1.5 Existing Policies

The specific privacy and security policies for MinID [15] states that Difi is responsible for treatment of personal data. The policy [7] also state that Difi is considered a data handler for personal information that is used to login to public services available through MinID. They are also responsible for information that is used to manage MinID. The eID policy states that Commfides and Buypass are responsible for handling the personal information needed to login using their provided systems. What this means is that Difi is not considered a data handler for all of the ID-portal, only their own solution.
The eID policy state that MinID only provides access to public services, but it is the service providers that are responsible for the personal information in their own services. This is interpreted as Difi not taking responsibility for information that is accessed using MinID, but stored in the systems of other service providers. Using MinID is also not mandatory, and the Norwegians may choose to not use MinID and stick to paper based solutions.

1.6 Value chain

Difi is a government owned body, and delivers authentication services. They measure values in the amount of users choosing the MinID solution for authentication in the ID-portal. This is also their main performance indicator for justification of funding from the Norwegian Ministry of Government Administration, Reform and Church Affairs (FAD). Figure 5 illustrates the most important value chain for Difi. Quality of service (QoS) affects the amount of users choosing MinID as their eID provider. The amount of users affects how much funding the Government is willing to delegate to Difi and the MinID project, which again regulates the amount of funding available for improvement of QoS.

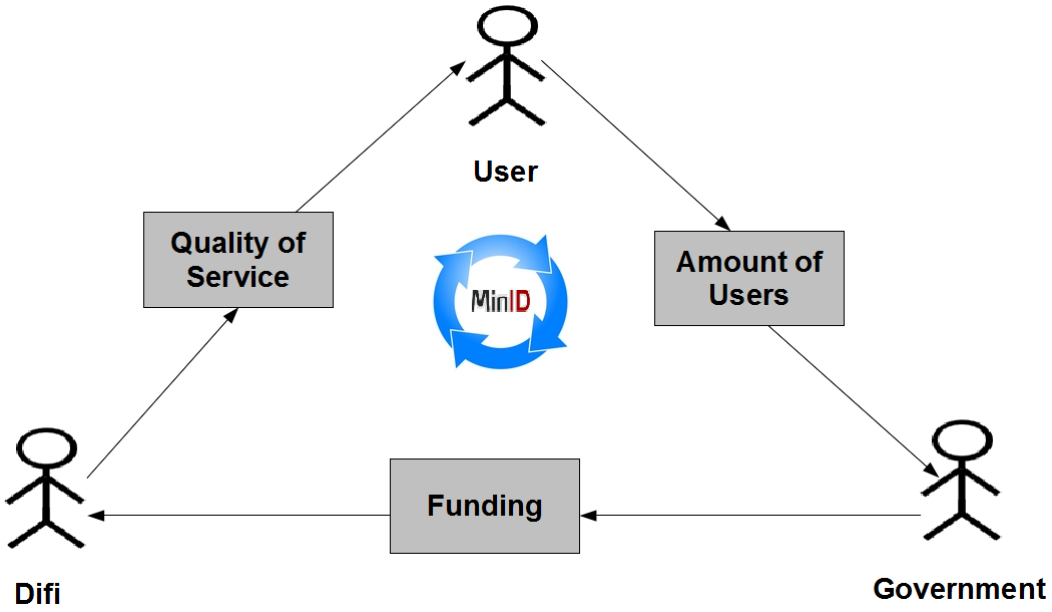


Figure 5: Main value chain for MinID

1.7 Risk Appetite, Tolerance and Culture

Without any interaction with Difi management, it is hard to estimate the appetite and the tolerance of the organization. Our estimate is that the enterprise's objective capacity to absorb loss is medium. This is a government funded non-profit organization, and therefore has a tight budget to stick to. A major incident will stretch their budget significantly, forcing them to save money in other areas. Bad publicity may also impact the amount of users choosing their solution for logging in to the ID-portal.
Since the organization deals with sensitive personal data [15], and is considered a data handler by Norwegian law [16], Difi is estimated to be a compliant organization since not being compliant can threaten the grounds of their own existence. Because of this reason and that they

facilitate access to many public services, and have a lot of users depending on their confidentiality, they are estimated to be risk averse.

2 Risk Scenario Identification

Risk IT does not specify a method for risk scenario identification other than top-down and bottom up scenario identification based on brainstorming and complete lists of threats, which is not sufficient for detecting risks to privacy. This chapter contains a top-down approach based data flow diagrams process modeling, which in the practitioners' opinions, suit the threat detection task better when looking for potential privacy risk scenarios in the MinID system. Non-privacy related weaknesses and vulnerabilities is not mentioned in this report as they are out of scope. All the identified privacy risk scenarios impacts the business goals in section 1.3 in some way.

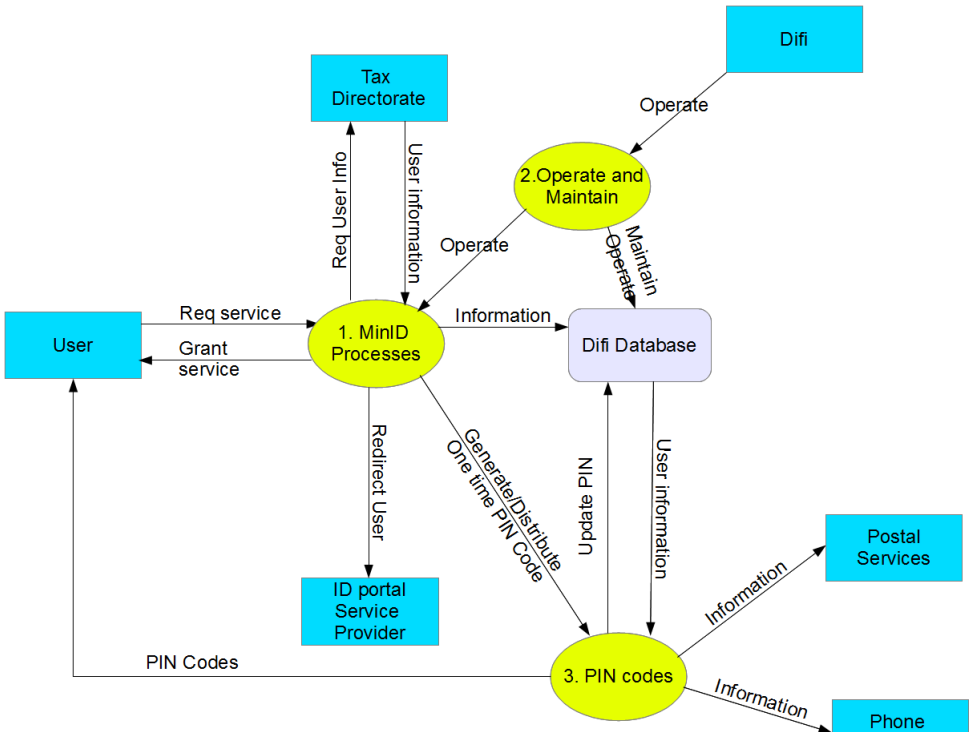
2.1 System Processes

The processes that is of interest in the system are those that handle personal data. The two models, figure 7 and figure 8, are based on the processes that handle personal data within the system. For each of these processes possible breaches on the data flows going in or out from the process will be analyzed to detect risk scenarios. A short explanation of the processes in the DFD is as follows:

1. Register new user: Unregistered user uses this process to register in the system. The process requires the user's SSN and personal data.
2. Fetch citizen data: This process uses the SSN to retrieve personal data registered about the user from the Tax Directorate Peoples register, and send it to the Difi Database.
3. Generate PIN Codes: Generates PIN codes for PIN letters users, and adds these to the letter from the Tax Directorate. It also adds the PINs to the Difi Database.
4. Send PIN letter: Is a process located in a third party, the postal services, which distributes PIN letters.
5. Authentication (Log in): Uses the SSN, password and PIN code for authentication. PINs are either from one-time PIN function or PIN letter.
6. Maintain Profile: Allows the user to maintain his personal data in the Difi Database. The personal data that can be updated is found in the yellow bubble in figure 4.
7. Generate One time PIN: This function generates a one time PIN for the user. This PIN is sent to the authentication process and the Mobile telephony service provider.
8. Check for Abuse/Error: This is the error and abuse checking process, it checks for inconsis-

tencies in the Difi Database and Difi High Level Database.

9. Send PIN code: Sends the one time PIN code to the registered cellphone number of the user.
10. Order New PIN-letter: Allows the user to order a new PIN letter.
11. Block PIN letter: This process blocks the PIN codes in the PIN letter. The user must now authenticate using one time PIN codes to the cellphone.
12. Account Service: is a process that can be contacted by the user for help with the account, either through cellphone or e-mail (possibly other means). This process is operated by humans that have access to the Difi databases.
13. Reset Password: This process helps the user reset a forgotten password.



v2/DFD0.png

Figure 6: DFD level 0

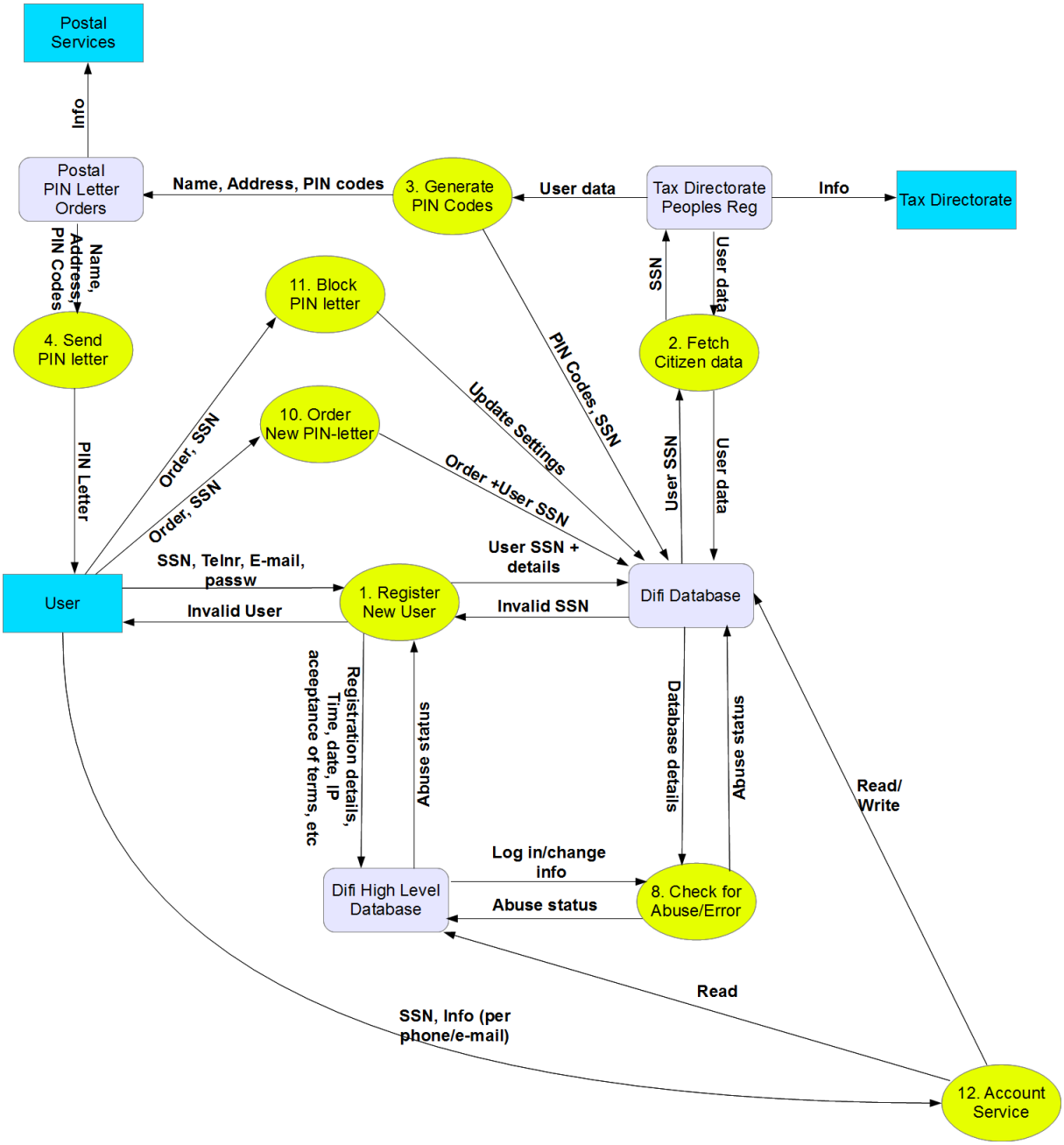


Figure 7: DFD process analysis 1

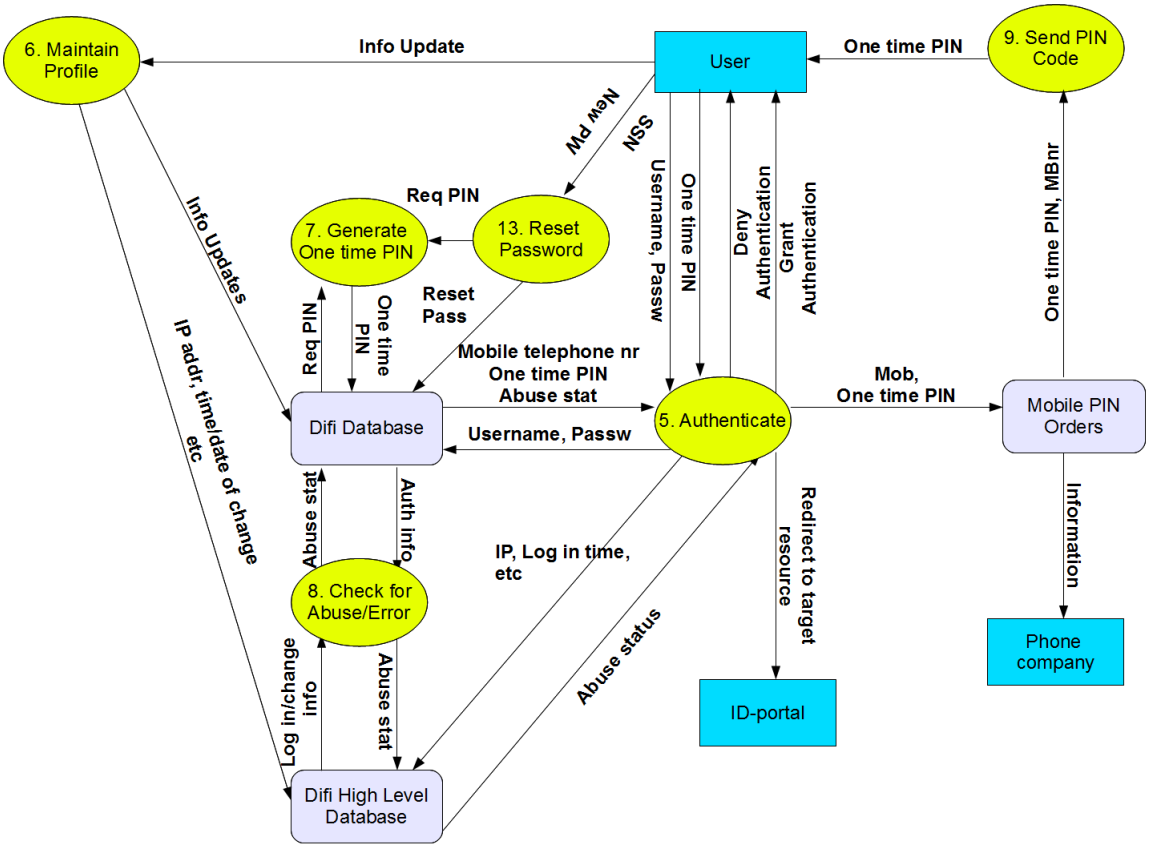


Figure 8: DFD process analysis 2

2.2 Identified Risk Scenarios

This section consists of the privacy risk scenarios that were detected using DFD analysis, for the complete analysis with all vulnerabilities see appendix 4.

1. External attacker breaches the confidentiality of the user's computer when registering for MinID, revealing SSN, chosen password, e-mail and mobile telephone number, identity theft using i.e. malware (or other computer attacks).
2. External attacker hijacks unregistered users' accounts through knowledge of victims SSN and postal address.
3. External attacker uses malware to compromise the user's computer and hijack the session when the user authenticates.
4. User is kept from his data due to a prolonged DoS attack on the service, leading to exclusion from his personal data.

5. Internal attacker reveals the data flows going in to the Difi database and the flow going out of the database, he can now data mine the data flows of SSN, passwords and one time PIN.
6. Internal attacker data mines first time registration detail flow going to high level database, and uses this information for aggregation.
7. Internal or external attacker compromises the process that collects data from the tax directorate, and manipulates input to data mine the tax register and/or corrupt the Difi database.
8. Internal or external attacker eavesdrops stream from the external tax register database to Difi database and data mines this stream.
9. External attacker reveals the content of the PIN letter and is able to reset the user's account password, hijacking the account.
10. External threats data gather the one-time PIN and telephone numbers when they are sent through mobile telephone services.
11. Mobile services collapse, creating a DoS for the users.
12. Hacker attacks compromise the Difi databases, leaking information about the users to the Internet.
13. Internal or external attacker compromises user sessions with ID-portal and gathers sensitive personal data.
14. Internal attacker eavesdrops information going to the high level database.
15. User is identified in the MinID system where he only needs to be authenticated and authorized.
16. Internal attacker manipulates the data stream to the high level database, causing a distortion of personal information.
17. Internal or external attacker manipulates data streams from profile maintenance, distorting information in the Difi Database.
18. System error causing the data flows into the databases to be corrupted, distorting database information about users.
19. Customer service accesses personal data for secondary use purposes.
20. Customer service accesses sensitive personal data in the high level database, for secondary use purposes.
21. External attacker wiretaps the customer service phone lines to obtain personal data.
22. External attacker uses phone phreaking vs customer service to obtain personal data about individuals.
23. External attacker exploits the reset password function together with obtained PIN codes to obtain access to accounts.
24. Mobile Phone company documents usage of MinID service, and uses it for surveillance or

profiling of customers.

25. Postal service company documents usage of MinID service, and uses it for surveillance or profiling of customers.

Some comments to the threat scenario identification:
There were too many scenarios to include them all, and many of them were similar. The guidelines from Risk IT framework were followed, and the amount of threat scenarios were reduced into a manageable set.

3 Risk Analysis

The risk analysis is conducted on the 25 privacy threat scenarios in section 2.2. Each scenario is analyzed in the adapted version of the Risk IT framework, with privacy in mind.

3.1 Privacy Risk Analysis

The "time" attribute was removed from the analysis because this is scenarios that can occur at any time and may have long time span. "Frequency" and "Magnitude" are indicated using the scale from 1-10, where 1 is low and 10 is highest. When defining magnitude, the results from the worst case privacy risks are used as an example. Frequency is described through likelihood of occurrence:

1. The risk is likely to occur 1/48 months or less.
2. The risk is likely to occur 1/36 months.
3. The risk is likely to occur 1/24 months.
4. The risk is likely to occur 1/12 months.
5. The risk is likely to occur 1/6 months.
6. The risk is likely to occur 1/3 months.
7. The risk is likely to occur 1 time each month.
8. The risk is likely to occur 1 time every other week.
9. The risk is likely to occur 1 time every week.
10. The risk is likely to occur multiple times each week.

Each risk is estimated using the frequencies outlined above according to the practitioners expertise. As a measure of impact the numbers from the taxonomy of privacy risks (see the main thesis) is used. Instead of assessing impact to the organization, this assessment uses a worst case impact to privacy. Each privacy risk scenario is classified within the taxonomy, and assigned the impact number of the most severe risk it presents. These numbers can be seen in figure 9.

Privacy Risk Impact assessment		
Privacy Risk	**Mean value**	**Privacy Impact**
1. Surveillance	7,7	Very High
2.Interrogation	6,6	High
3. Aggregation	6,5	High
4. Identification	8,2	Very High
5. Insecurity	8,6	Very High
6. Secondary use	7,8	Very High
7. Exclusion	8	Very High
8. Breach of Confidentiality	8,4	Very High
9. Disclosure	8,3	Very High
10. Exposure	7,8	Very High
11. Increased Accessibility	6,6	High
12. Blackmail	8,3	Very High
13. Appropriation	7	High
14. Distortion	7,5	Very High
15. Intrusion	6,4	High
16. Decisional Interferens	6,2	High
17. Denial of Anonymity	6,9	High
18. Function Creep	7,9	Very High
19. Legal Consideration	7,8	Very High

Figure 9: Privacy Risk Impact

Scenario nr	Actor	Threat Type	Event	Asset	Privacy threat	Frequency	Frequency comments	Magnitude	Risk Classification
1	External	External Requirement	Inappropriate use	Customers	Insecurity	7	Hacking of Pcs occur daily, and account hijacking is likely to happen	8,6	Really Unacceptable
2	External	Malicious	Ineffective design	Customers	Secondary use, Function creep	5	The howto on using this attack is not hidden and is likely to occur	7,9	Unacceptable
3	External	Malicious	Ineffective design	Customers	Insecurity	4	Attack is possible but requires knowledge of vulnerabilities.	8,6	Unacceptable
4	External	Malicious	Interruption	Customers	Exclusion	2	DoS is not likely to occur over a significant time period	8	Unacceptable
5	Internal	Malicious	Inappropriate use	Customers	Insecurity	2	Not a likely target for attack for an insider. Value of target is not high.	8,6	Unacceptable
6	Internal	Malicious	Ineffective design	Customers	Aggregation	2	Not a likely target for attack for an insider. Value of target is not high.	6,5	Acceptable
7	Internal/External	Malicious	Modification	Customers	Distortion	2	Not a likely target for attack for an insider or outsider.	7,5	Acceptable
8	Internal/External	Malicious	Disclosure	Customers	Surveillance	3	Data stream is likely to be encrypted and well secured.	7,7	Unacceptable
9	External	Malicious	Ineffective design	Customers	Insecurity	5	Many mailboxes in Norway lacks security	8,6	Really Unacceptable
10	External	Malicious	Ineffective design	Customers	Surveillance, Denial of anonymity	8	External SP are very likely to have logs of service use, that can be abused outside of Difi's control	7,7	Really Unacceptable
11	External	Failure/Natural	Interruption	Customers	Exclusion	4	Telephony infrastructure is vulnerable for short periods of downtime due to natural disasters	8	Unacceptable
12	External	Malicious	Theft	Customers	Insecurity, Disclosure	2	A likely target for attack, but the database is well protected.	8,6	Unacceptable
13	Internal/External	Malicious	Disclosure	Customers	Insecurity	5	Session hijack is possible through browser weaknesses.	8,6	Really Unacceptable
14	Internal	Malicious	Theft	Customers	Insecurity	7	A likely target for attack by the insider.	8,6	Really Unacceptable
15	Internal	Malicious	Ineffective design	Customers	Denial of Anonymity	10	This happens through the use of SSN as identifier	6,9	Really Unacceptable
16	Internal	Malicious	Destruction	Customers	Distortion	2	Not a likely target for attack for an insider.	7,5	Unacceptable
17	Internal/External	Malicious	Destruction	Customers	Distortion	1	Not a likely target for attack for an insider or outsider.	7,5	Acceptable
18	Internal	Accidental/Error	Destruction	Customers	Distortion	3	The odd software and hardware errors are likely to occur once in a while	7,5	Unacceptable
19	Internal	Malicious	Disclosure	Customers	Secondary use	5	When the opportunity for abuse of personal data is present, it is likely to be exploited	7,8	Really Unacceptable
20	Internal	Malicious	Disclosure	Customers	Secondary use	4	When the opportunity for abuse of personal data is present, it is likely to be exploited	7,8	Unacceptable
21	External	Malicious	Disclosure	Customers	Insecurity	2	Wiretaps is an unlikely attack vector.	8,6	Unacceptable
22	External	Malicious	Disclosure	Customers	Insecurity	6	Phone phreaking is a low risk, cost effective and common way of attacking	8,6	Really Unacceptable
23	External	Malicious	Ineffective design	Customers	Insecurity	6	This attack does not require intricate knowledge of the system to figure out, and is a likely attack path.	8,6	Really Unacceptable
24	External	Malicious	Ineffective design	Customers	Surveillance, Denial of anonymity	8	Difi have no control of what SP does with the information it recieves. This is an easy accessible source of information	7,7	Really Unacceptable
25	External	Malicious	Ineffective design	Customers	Surveillance, Denial of anonymity	4	Difi have no control of what SP does with the information it recieves. But this is a slow process.	7,7	Unacceptable

3.2 Risk Level

Risk level is defined from the frequency and magnitude results. Acceptable risk means that the risk is so small that introducing mitigating measures or strategies, will not be profitable. Unac-

ceptable risk means that the privacy risk scenario is above the threshold for what is acceptable, and must be handled immediately. Each scenario in figure 10 is indicated by its number from section 2.2.
The different risk levels used are:

- Red - Indicates that a risk is severe, and should be dealt with immediately.
- Yellow - Indicates that a risk is above the risk appetite, and should be dealt with.
- Green - Indicates that the risk has a normal risk level, and does not need any risk reducing measures.
- Blue - Indicates very low risk, and that there might be opportunity for the organization to increase risk in this area, to i.e. decrease security measures to increase business effic

Some of the illustrated risks in figure 10 have the same values, but are placed slightly different in the matrix, this is done to avoid stacking the different risk scenario numbers on top of each other and for readability.

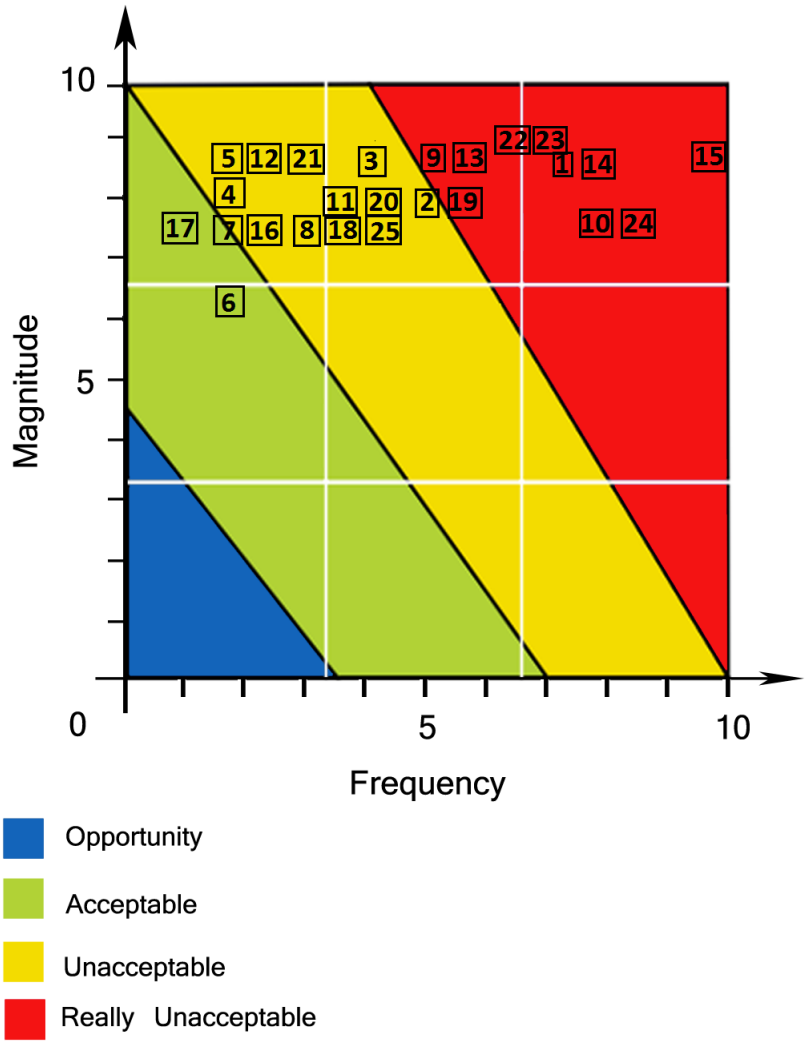


Figure 10: Risk Level

Bibliography

[1] 2009. The risk it practitioner guide.

[2] 2009. The risk it framework.

[3] 2010. To millioner kan legge bort pin-kodene. http://www.difi.no/artikkel/2010/04/to-millioner-kan-legge-bort-pin-kodene. (Visited Feb. 2012).

[4] 2012. Om difi. http://www.difi.no/om-difi.

[5] 2011. Difi - organisasjonskart. http://www.difi.no/om-difi/organisasjonkart. (Visited april 2012).

[6] Ølnes, J. 2012. Evolution of minid and the id portal, lecture. https://wiki.uio.no/mn/ifi/AFSecurity/index.php/Main_Page. Lecture held in UiO, 250112, AF Security.

[7] 2011. Minid - sikkerhet og personvern. http://www.difi.no/elektronisk-id/minid/sikkerhet-og-personvern.

[8] D-nummer. http://www.skatteetaten.no/no/Alt-om/Folkeregistrering/D-nummer/. (Visited Feb 2012).

[9] 2010. Sikkerhet og personvern. http://www.difi.no/elektronisk-id/sikkerhet-og-personvern.

[10] Østvold, B. M. 2010. Case study - privacy-relevant information flow in information management systems. http://petweb2.projects.nislab.no.

[11] 2012. Sikkerheit og funksjonalitet. http://www.difi.no/artikkel/2011/11/sikkerheit-og-funksjonalitet. (Visited feb 2012).

[12] Oasis security services (saml) tc. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security. (Visited Feb. 2012).

[13] Openam. http://forgerock.com/openam.html. (Visited March. 2012).

[14] Open directory service. http://www.opends.org/. (Visited March. 2012).

[15] Privacy and security. http://minid.difi.no/minid/personvern.php?lang=en. (Visited feb 2012).

[16] 2000. Personal data act. http://www.lovdata.no/all/hl-20000414-031.html. (Updated 2009).

4 Appendix 1: Complete DFD Risk Identification Analysis

Process nr + Name	**Data flow name**	**Availability** (Column two is used to indicate privacy threat)		**Confidentiality** (Column two is used to indicate privacy threat)		**Integrity** (Column two is used to indicate privacy threat)	
1. Register New User	SSN, Telnr, E-mail, passw	- Cutting this can lead to DoS Ext attacker: can be done with a DdoS vs the user. This presents no imminate privacy risk, DoS must be prolonged to a amount of time to qualify as «Exclusion».	No	- Breaching the C(onfidentiality) of dataflow can be used to reveal User info. Can be done by breaking encryption and eavesdropping, or malware.	Yes	- Attack on this flow can allow the attacker to hijack the session. Can be accomplished on unregistered users, and through technical attacks.	Yes
	Invalid User	- Cutting this flow would only deny the user his invalid log in information. Ext attacker: DdoS vs server.	No	- Breaching the C of this dataflow can yield information about the registration status of the user. Eavesdrop or Malware	Yes	- Being able to compromise this flow will make the attacker able to DoS the User. Compromising the server, or hijacking server.	No
	User SSN + details	- This flow carries info to the difi database, and users would not be able to register, creating DoS. Int attacker compromising dataflow or process.	No	- Breaching the C of dataflow can be used to reveal User info. Can be done by breaking encryption and eavesdropping. Internal attacker can eavesdrop this flow.	Yes	- Compromising this dataflow will allow an attacker to modify registration details, such as mobiletelephone nr, e-mail and chosen passw, effectively hijacking the account. Internal attacker can breach dataflow.	Yes
	Invalid SSN	- Cutting this dataflow will only ultimately deny the registration process information about the user's registration status, creating a DoS.	No	- Breaching the C of this flow will only reveal registration status. This flow carries information about the users registration status, and is no threat in it self, but the information can be exploited in a combination of information.	No	- Compromising this dataflow will allow the attacker to manipulate the registration status of the user, feeding the user false information. Man in the middle attack-	No
	Registration details	- Cutting this dataflow will deny the high level database registration details, these details are not critical for the system.	No	- Revealing the content of this flow will reveal registration details of the user (including location). This can be done through compromising the high level database, or eavesdropping the flow.	Yes	- Attack on this dataflow will allow the threat agent to manipulate registration details of the user. Potentially hiding account abuse.	No
	Abuse Status	- Cutting this dataflow would help an attacker hiding abuse of the system. But is a small threat in itself.	No	- Revealing the content of this flow would only give away if the new user's abuse status.	No	- Attack on this dataflow will allow an attacker to either hide his tracks or to create a DoS for the user trying to register, as flipping this stream to abuse for everyone will deny access. Man in the middle attack.	No

2. Fetch Citizen Data	SSN	- Cutting this dataflow will deny the system the opportunity to obtain user data creating system error and DoS.	No	- Copying the content of this dataflow would reveal SSN and that user is unregistered in the system. Hacker attacks	Yes	- Manipulating this dataflow will allow the attacker to retrieve information about other people from the tax register, creating an error in the system, or DoS. Hacker attacks.	Yes
	User data (from Tax)	- Cutting this dataflow will deny the system user information, creating a DoS and error.	No	- Copying the content of this dataflow would reveal user data from the Tax register. Hacker attacks, External attacks	Yes	- Manipulation this dataflow will allow for changing details from the tax register, corrupting the Difi Database. External computer attacks	Yes
	User data (to DB)	- Cutting this dataflow will deny the system user information, creating a DoS and error.	No	- Copying the content of this dataflow would reveal user data from the Tax register. Hacker attacks, Internal attacks	Yes	- Manipulation this dataflow will allow for changing details from the tax register, corrupting the Difi Database. Internal computer attacks	Yes
	User SSN	- Cutting this dataflow will deny the system the opportunity to obtain user data creating system error and DoS.	No	- Copying the content of this dataflow would reveal SSN and that user is unregistered in the system. Hacker attacks	Yes	- Manipulating this dataflow will allow the attacker to create an error in the system or DoS. Hacker attacks.	Yes
3. Generate PIN codes	User data	- Cutting this flow will deny the user his PIN codes, and denying him access to the system.	No	- Copying the content of this dataflow will reveal name, address and that the user uses MinID. This can also be found on the internet, and a little under 50% of the Norwegian population uses MinID.	No	- Manipulating this datastream will allow the attacker to manipulate user data of the PIN code generation, allowing the attacker to generate PIN codes for other users in the system.	Yes
	Name, Address, PIN Codes	- Cutting this flow will deny the user his PIN codes, and denying him access to the system.	No	- Copying the information of this flow will reveal the Name, address and PIN codes of the user, but the attacker will still lack password. Two factor attacks.	Yes	- M(anipulating) this datastream will allow the attacker to manipulate name and address of the PIN code shipment. Hacker attacks.	Yes
	PIN codes	- Cutting this flow will deny the MinID database PIN codes, creating an error in the system and probable DoS for the user.	No	- This flow will reveal the SSN and corresponding PIN codes of the user. Internal hacker attacks.	Yes	- M of this datastream will allow the attacker to overwrite PIN codes of other users by manipulating the SSN. It also opens for manipulations of PIN codes of the registering user, and corruption of the database. Internal hacker attacks.	Yes

4. Send PIN letter	Name, Address, PIN Codes	- Deny the system details for PIN letter, effectively DoSing the user.	Yes	- Eavesdropping this dataflow will reveal PIN-codes, name and address of the user. External malicious employee	Yes	- M this datastream will allow the attacker to manipulate name and address of the PIN code shipment. Hacker attacks or external malicious employee.	Yes
	PIN Letter	- Pin letter getting lost in mail or something similar will delay the user's access to the system.	No	- Opening the PIN-letter will reveal the PIN codes of the user. If the user is unregistered, the PIN codes and the SSN can be used together to create the MinID accout. ID-theft. External attacker exploit.	Yes	- M this datastream will allow the attacker to readdress the letter or manipulate letter content. Will allow the attacker to manipulate the codes and DoS the user. External attacker.	No
5. Authenticate	Username, Passw (from user)	- Cutting this flow will create DoS for user. External attacker	No	- Will reveal Username/pass, but still lack PIN codes for two factor authenticaiton. External attacker, malware	No	- Only create DoS for user. External attacker.	No
	One time PIN	- Cutting this flow will create DoS for user. External attacker	No	- Will reveal the one time PIN, but this is useless without the username/pass to go with it. External attacker, malware	No	- Only create DoS for user. External attacker.	No
	Deny Authentication	- Prevent user from obtaining reasons for beeing denied access to system.	No	- Reveal reasons for denied authentication.	No	- Compromising this datastream will only act as a nuisance for the user.	No
	Grant Authentication	- Prevent user from authenticating with the system. (Exclusion) External attacker, malware	Yes	- Reveal content of granted authentication stream.	No	- Possibility for session hijack. External attacker	Yes
	Mob, One time PIN	- Prevent user from authenticating, DoS. External/interal attacker	No	- Revealing content of the one-time PIN message will reveal the PIN and telephonenumber of the user. Can be used in aggregation. External/inter attackers	Yes	- M the one-time PIN to be sent to a different mob number. DoS or part of account hacking attack. Internal/external attacker	Yes
	Redirect to target resource	- Prevent the user from accessing the target resource in the ID-portal. DoS.	No	- Revealing the contents of this datastream can reveal sensitive personal information about the user. Internal attacker.	Yes	- M and modifying this datastream can reveal sensitive information about the user. Internal attacker.	Yes
	Abuse status	- Prevent the authentication process from detecting account abuse. Internal attacker/external attacker	Yes	- Revealing the content of this stream will not disclose any personal information.	No	- M the abuse dataflow will effectively disable the defence an enable a prolonged attack.	No

	IP, Log in time, ...	- Prevent the high level database from compiling information for detecting account abuse. Internal attacker/external attacker	Yes	- Revealing this information flow can allow an attacker data gathering on the users. Internal attacker	Yes	- M this dataflow will effectively disable the defence an enable a prolonged attack. It will also distort the information in the high level database. Internal attacker	Yes
	Username, PW (DB)	- Preventing this flow will create a DoS for the user	No	- Revealing this data flow will reveal username and pass of the user.	No	- M this dataflow will only create a DoS for the user by itself.	No
	Mobtlp, onetime PIN, abuse stat (DB)	- Preventing this flow will create a DoS.	No	- Revealing this stream will reveal telephonenr and one time PIN. Telephone nr is a unique identifier and can tie the user to the system and SSN. Internal attacker.	Yes	- M this dataflow can allow the attacker to send the one-time code to antoher telephone nr, DoSing the user and facilitating an account hack. Internal attacker.	Yes
6. Maintain profile	Info updates (User)	- prevent the user from updating his own information. Exclusion Internal / external attacks	Yes	- Eavesdropping this information stream would reveal personal data. Disclosure Computer attack	Yes	- M this information stream can casue distortion of personal data. Internal/external attacker	Yes
	Infor updates (DB)	- P(revent) the user from updating his own information. Exclusion External attacks	Yes	- Eavesdropping this information stream would reveal personal data. Disclosure Computer attack	Yes	- M this information stream can casue distortion of personal data. Internal/external attacker	Yes
	IP addr, + info	- P the High level DB from attaining information from profile changes will cause a corruption (distortion) of data in DB.	Yes	- E(avesdropping) this information stream would yield IP addr, time/date of change. Can be used for Surveillance. Internal attacks.	Yes	- M would cause a corruption of Highlevel DB info, and distortion of DB data.	Yes
7. Generate One time PIN	Req PIN (13.)	- Would deny the processes and ultimately the user getting his PIN code. DoS.	No	- E the PIN req would not yield valuable information.	No	- M would only deny the user PIN codes. An attacker can probably cause damage to the system, but not to privacy.	No
	Req PIN (DB)						
	One time PIN	- P the One time PIN flow would only create a DoS	No	- E the one time PIN would yiled the one time PIN, but there are more likely places to attack than this.	No	- DoS. In itself, having access to M this dataflow does little for an attacker when the target is privacy.	No
8. Check for Abuse/Error	Abuse stat	- P the abuses stat flow will disable messages from the security system in process 8. Opening for attacks on the system. Internal attacks.	Yes	- Will not yield anything useful.	No	- M of this flow can be used to hide attacks on the system.	No
	Auth Info	- Cutting this will only partially disable the security system, due to two dataflows going into the error check.	No	- Will yiled authentication information, but not much useful.	No	- M of this flow can be used cover abuse of the system, but presents no immediate threat to privacy.	No

	Log in, Change info	- This will cut off the security system connected to the high level database, can be used to help prevent abuse, but does not prevent any threat to privacy.	No	- E on this flow will yield personal data that can be used for surveillance of an individual.	Yes	- M of this information flow can help hide an attack by disabling the highlevel security system.	No
9. Send PIN Code	One Time PIN, Mbnr	- Cutting this flow can DoS the user, but he can bypass this with PIN letter.	No	- If an attacker E this dataflow he will reveal the user, and that he uses this service. Denial of anonymity, surveillance External attacker.	Yes	- M of this dataflow, attacker can reroute the PIN code to himslef as a part of the attack.	No
	One time PIN	- Cutting this flow can DoS the user, but he can bypass this with PIN letter.	No	- If an attacker E this dataflow he will reveal the user, and that he uses this service. Denial of anonymity External attacker.	Yes	- M of this dataflow allows the attacker to manipulate message content.	No
10. Order New PIN letter	Order, SSN	-DoS.	No	- This will only reveal that SSN need new PIN-letter.	No	- M of this flow will only be regarded as nuisance.	No
	Order + User SSN	-DoS.	No	- This will only reveal that SSN need new PIN-letter.	No	- M of this flow will only be regarded as nuisance.	No
11. Block PIN letter	Order, SSN	- No threat.	No	- This will only reveal that the user has chosen the mobile solution.	No	- M of this flow will only reactivate PIN letter .	No
	Order, SSN	- No threat.	No	- This will only reveal that the user has chosen the mobile solution.	No	- M of this flow will only reactivate PIN letter .	No
12. Account Service	Read/Write	- No threat to privacy by cutting this connection. It may strengthen privacy	No	- E this flow can reveal personal data. Insecurity, surveillance, Breach of confidentiality Internal attackers	Yes	- M of this flow can distort personal information information	Yes
	Read	- No threat to privacy by cutting this connection. It may strengthen privacy	No	- E this flow can reveal sensitive personal data. Insecurity, surveillance, Breach of confidentiality Internal attackers	Yes	- M of this flow can distort personal information information	
	SSN, Info	- Disruption of customer service will be quicly detected. \	No	- Wiretap can reveal personal information about the user. External attackers	Yes	- Phone phreaking using name and SSN can be used to alter information in the database and ID-theft. External attackers.	Yes

13. Reset Password	SSN, New PW	- DoS	No	- Obtaining SSN and corresponding new PW is useful. External attacker, Malware	Yes	- Useful for account hijacking. But the one-time PIN is still needed for full control. External attacker, Malware	Yes
	Req PIN	- Would deny the processes and ultimately the user getting his PIN code. DoS.	No	- E the PIN req would not yield valuable information.	No	- M would only deny the user PIN codes. An attacker can probably cause damage to the system, but not to privacy.	No
	Reset Pass	- DoS	No	- Obtaining SSN and corresponding new PW is useful. Internal attacker	Yes	- Useful for account hijacking. But the one-time PIN is still needed for full control. Internal attacker	Yes
Misc dataflows	Mobile PIN orders – Information to Phone company	- No threat.	No	- This data yields information about individuals which the phone company does not need to have. Denial of anonymity, secondary use, identification	Yes	- Distortion of personal data External attacker	Yes
	Postal Services – Info	- No threat	No	- This data yields information about individuals which the Postal services does not need to have. Denial of anonymity, secondary use, identification, information collection.	Yes	- Distortion of personal data External attacker	Yes
	Tax Directorate – Info	- No threat	No	- This data yields information about individuals which the Tax Directorate does not need to have. Denial of anonymity, secondary use, identification, information collection.	Yes	- No threat.	No

C Appendix - Complete Scenario Description

This is appendice contains the complete scenario description used for this thesis, including a detailed description of each stakeholder.

The case study in this project is based on the MinID identity managemet system provided by the Norwegian Agency for Public Management and eGovernment (Difi). MinID is a part of the federation called "ID-portal" (ID-porten) which can be logged into using MinID, or other eID providers. The ID-portal facilitates access to public services like tax, health services and many others. In april 2010, the number of registered norwegian citizens using MinID increased to over 2 million users [45].

C.1 Scenario background

According to Jon Ølnes (lecture AF Security seminar, University in Oslo 25.01.2012) Difi views a person's electronic identity as "... the collection of all electronic information that can be attributed to the person" [56]. The scope of this scenario will be privacy and the system's handling of privacy sensitive information. This case first provides a description of MinID as a system, and the different functionalities of the system. The next part consists of a stakeholder analysis.

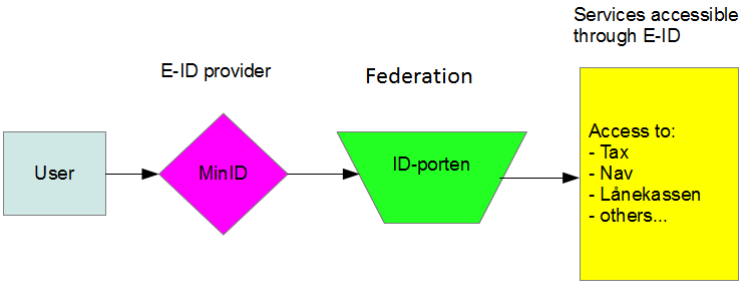


Figure 43: Illustration of how ID-porten and MinID works.

To log in using MinID, the user applies his Norwegian social security number (fødselsnummer, consists of 11 numbers) or D-number (temporary number given to foreign citizens that pay taxes to Norway) [59], a personal password and a one-time PIN code. The PIN code is either

found on piece of paper containing several codes delivered by mail, or it can be sent to the user's mobile telephone if he/she has registered the telephone number. The latter is becoming the more common solution [3],as paper is regarded as an old-fashioned solution.

C.1.1 Difi Objectives

Difi is an organ of the Norwegian government, and their vision is "We develop the public sector" [3]. Difi aims to contribute to the public sector by renewing and developing it, and strengthen cooperation between vendors and offer joint solutions.
Their goal concerning electronic identities is to establish a joint infrastructure for use of electronic identities in governmental sectors [56]. To achieve this objective they have developed the solution known as MinID. The main objective of MinID is to ensure access to governmental services through the use of electronic identities in a secure way [42]. One of the main reasons for implementing ID-porten and MinID is the amount of time and money that can be saved through digitalization of the public services.

Other Difi goals are [56]:

- The public sector will use Difi's knowledge, means and tools, something which is achievable only through cooperation and dialog.
- Good cooperation with the rest of the government is the most important prerequisite for our success.
- Difi has a special responsibility for the renewal and development of public sector in the areas of ICT, procurement, communication, organization, instruments and training.
- Transactions between citizens and the government should mainly be digitalized.
- Digital solutions shall be offered for all suitable governmental services.
- Digital services shall be shaped by the user's need and be secure and effective.
- MinID is to be based on open source solutions.
- Handle foreign logins.

C.1.2 MinID purpose and functionalities

MinID is an identity management system that holds access credentials for Norwegian citizens, and provides authentication for accessing many services provided by the Norwegian Government such as:

- Altinn.no - site for handing in electronic schemes for public services.

- brreg.no - National registers in Bronnoysund.
- lanekassen.no - Unit for financial support for students.
- NAV.no - The Norwegian Labour and Welfare Administration.
- samordnaopptak.no - Norwegian Universities and Colleges Admission Service.
- Posten.no - Norwegian Postal services.
- Norwegian municipalities and counties.
- Others [60].

One of the possible use cases of MinID is illustrated in figure 43. The illustration shows how MinID can be used to gain access to public services through the ID-portal federation. "eID providers" can also refer to Commfides and Buypass developed solutions, which are two other alternatives for logging into ID-porten. This is one of the three main tasks for which MinID can be used. According to Ølnes [56], it can also be used to *digitally sign and verify documents*, and to *facilitate encryption and decryption*. These two functionalities, together with handling foreign logins, are out of scope for this thesis.

C.1.3 MinID, expectation and regulations by the Norwegian Government

eNorway2009 [64] and Stortingsmeldingen number 17 [65] (St.m 17) contains the political vision of improving the efficiency of Norwegian governance. St.m 17 describes ICT as a possibility that can lead to societal gains, if approached with a cooperation between public sector, private sector, citizens and the government.
The three main target areas for this initiative [64], is the individual in the digital Norway, innovation and growth in business and industry, and a coordinated and user-adapted public sector. Ambitions include better and more effective utilization of public resources, and improved public services. The government also aimed to include ICT in education, and prioritize availability of public services for everyone. MinID was developed as a part of this commitment to ICT, and the vision of a digitalized Norway.

In 2005, Difi defined specifications for establishing a public key infrastructure (PKI) in Norway, which was later approved by the Norwegian government [57]. The specifications were later updated and the newest version is from 2010 [58]. These specifications are the basis for regulation of requirements of eID and e-signature. Which means that MinID also is bound by these specifications.
The purpose of these specifications is to provide a basic guidance for what is required by the government when implementing PKI-solutions. It also works as a means to standardize PKI services within the management. More about specification for PKI in public sector can be found here [58].

The Norwegian government has also published a framework for facilitating online services and collaboration for public services called "Framework for authentication and non-repudiating in electronic communication with public sector" [66]. This document includes demands and what to be expected of the presented electronic solution. The framework is meant to help facilitate the reuse of authentication solutions and reduce the number of authentication solutions needed.
The government operates with four different levels of security, one being lowest and four highest (the definitions of each level of security can be found in document [66]). MinID can be used for authentication up to security level 3 [56, 67]. The reasons for MinID being level three instead of four, is that the user only needs to have a Norwegian social security number (SSN) to obtain codes for logging in. Solutions such as Buypass and Commfides demands that the user shows up personally and identifies him/herself when collecting the authentication devices [67].

C.1.4 Laws and regulations

MinID is a Norwegian IdMS, and is therefore bound by Norwegian laws and legislations. MinID also handles sensitive personal data and is therefore subject to the "Personal data act" [18] and the "Personal data regulations" [19]. The purpose of the act and regulation is to protect individuals from having their privacy violated, and it should also contribute to the security of handling personal data and strengthen privacy [18].
Since Difi is a subject to the Norwegian government, there exists an act that constitutes right of access to documents, journals and the likes in public administration for Norwegian citizens [43] (Offentleglova), for which Difi must be compliant. This means that the goal of being as transparent an organization as possible is founded in the law. The law of goveranace [47] is applicable to the activities of all departments within the state or local government of Norway.

MinID is also subject to the "E-signature act" [68]. The purpose of this act is to facilitate secure and effective use of electronic signatures, and is mainly directed at certificate issuers. This is accomplished by setting requirements for the qualified certificates, the issuer of the certificates and the secure signature creation devices. The "E-governance regulation" [69] is a regulation developed to facilitate secure and effective use of electronic communication with and in the governance. It is meant to emphasize predictability and flexibility within technical solutions.

C.1.5 MinID privacy policies

The specific privacy and security policies for MinID [62] states that Difi is responsible for personal data, and is considered a data handler. The privacy policies for electronic ID [61] and MinID [42] are similar, but the one for electronic ID (eID) is more extensive. The eID policy is interpreted to apply for all the eID providers in the ID-portal, while the latter is specific for MinID.
The policies state that Difi is considered a data handler for personal information that is used to login to public services available through MinID. Difi is also responsible for information that is used to manage MinID. The eID policy states that Commfides and Buypass are responsible

for handling the personal information needed to login using their provided systems. What this means is that Difi is considered a data handler only for their own solution, and not for all of the eID providers in the ID-portal.
The eID policy state that MinID only provides access to public services, but it is the service providers that are responsible for the personal information in their own services. This is interpreted as Difi not taking responsibility for information that is accessed using MinID, but stored in the systems of other service providers. Using MinID is also not mandatory, and the Norwegians may choose to not use MinID and stick to other solutions.
Although similar, the two eID policies are also conflicting in some areas, the policy for eID states that the system forwards social security number and login information, while MinID policy states that the system forwards social security number and language choice. What "login information" means is unclear. Another conflict between the two statements is in regard to the logging of log ins for each user. The MinID policy states that they keep logs to protect the user against abuse and error, while the eID policy states no reason for having these logs other than for statistical purposes.

C.2 The MinID IdMS

In the view of the system that was used in this case, a distingtion is made between the information actually present in the MinID IdMS, and the information it provides access to. The system is illustrated in a top-down view in figure 44. The figure represents the different parties directly involved with MinID. The purple rectangle in the middle represent the main services offered by MinID. And the pale yellow rectangles are service providers directly in contact with the MinID system. The encryption/decryption and eSignature functions are not considered as a part of the scope in this project. A short explanation of the figure:
The purple rectangle in the middle includes the services provided by MinID. MinID has several contact points, the User (represented by the stick man) can use the services provided by MinID. If the user authenticates through MinID to use any public services, the personal data accessed after entering the website of the service provider (Tax, NAV, etc...) is outside of the scope of this case study. This was because of the privacy statement mentioned earlier by Difi [61] which states that the public services are responsible for the personal data in their own systems. The Tax directorate holds citizen data about all Norwegian citizens with a social security number, and is in direct contact with MinID when new users are registered [61]. The tax directorate is also the handler of PIN letters [62], these are ordered on the MinID portal provided by Difi. MinID sends one time PIN code through the Phone Company back to the user.

The system depicted in figure 24 is illustrated according to descriptions gathered from open sources. The personal information the system handles, are social security numbers, PIN-codes, passwords, e-mail addresses, telephone numbers and logs containing usage of MinID for each user. What has been gathered about the content of these logs is depicted in figure 45, the content illustrated has been confirmed present, but there is a possibility that the logs contain more in-

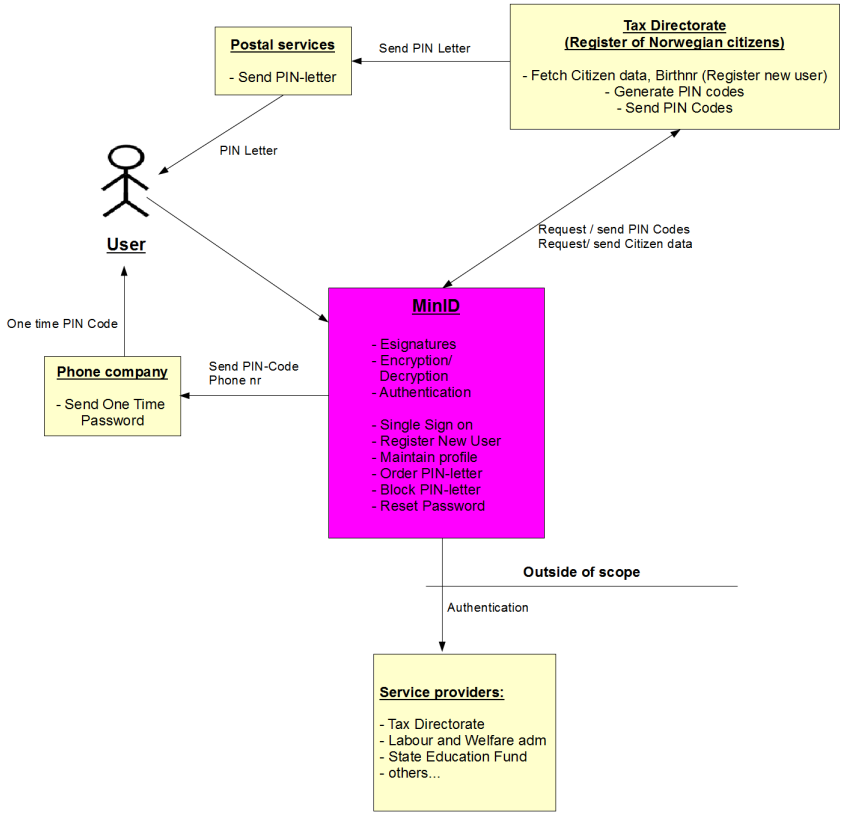


Figure 44: MinID IdMS

formation about the user (sources difi website [2, 42, 62] and Appendix F). Difi is characterized as a data handler according to Norwegian law [18]. MinID passes on social security number and chosen language to the service provider.

C.2.1 Technology and solutions

According to Østvold and Difi's website [44, 70], the design of ID-porten is based on the OASIS SAML 2.0 standard for web services [71], OpenAM from ForgeRock AS [72], and the OpenDS Directory Sever [73]. OASIS SAML 2.0 is, according to their website, an open standard for single sign on systems. When authenticating using MinID, the one time PIN code can, as previously mentioned, be found on a PIN-letter from postal services. Or the a one time PIN-code can be sent to the user, using mobile telephone services. The authentication proceedure using mobile telephony together with the SSN and personal password is illustrated in figure 46.

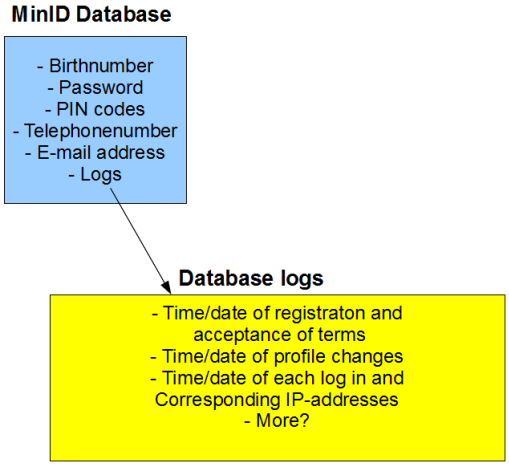


Figure 45: Personal data in high level database.

C.3 Stakeholders, MinID

There are many different stakeholders involved in MinID. To get an overview of the stakeholders related to MinID, they have been categorized using a top-down approach, illustrated in figure 47. Where class 1 is a general classification of the type of stakeholders, and class 2 is more specific. Class 3 is not represented in the figure, but are represented in the following stakeholder analysis (colors are for illustrative purposes to indicate levels). This chapter contains an introduction and description of the stakeholders, as well as a summary of the analysis. The complete stakeholder analysis can be found in the appendix D.

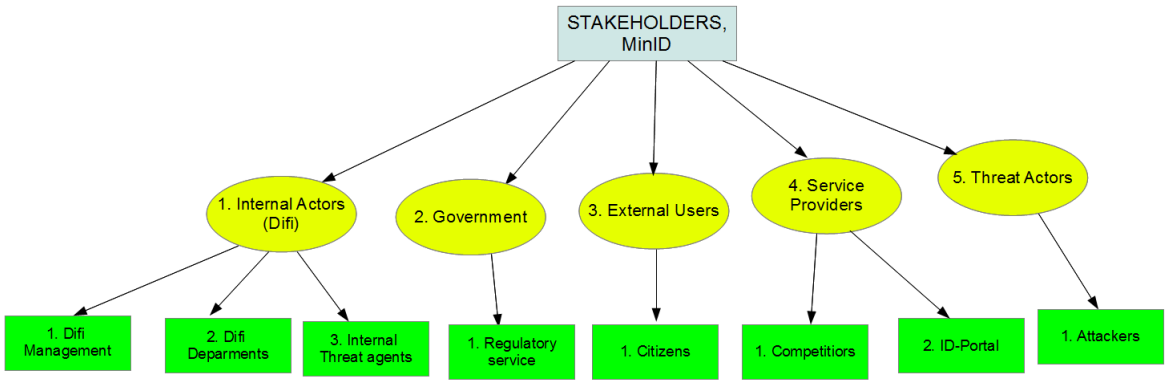


Figure 47: Categorization of stakeholders class 1 and 2.

The methodology for the stakeholder identification and basic analysis is found in section 4.2.2. The stakeholders that have been identified as important for this case are listed and analyzed in

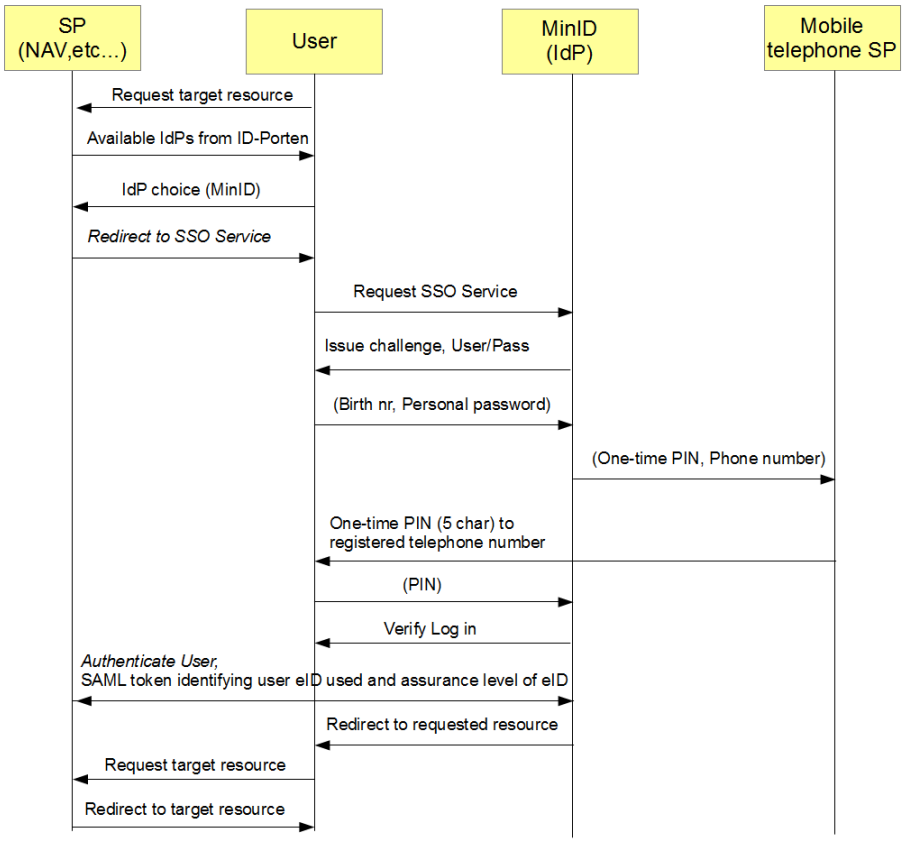


Figure 46: Authentication proceedure MinID

this chapter. One important thing to mention is that each stakeholder has more capabilities and assets than is portrayed in this analysis, an attempt has been made to select the most important capabilities and assets regarding privacy the analysis, and reduce them to a manageble set.
The different categories and their corresponding sub-categories will be addressed as in their own sections and sub-sections. The number of level three stakeholders to be analyzed have been limited to eight.

C.3.1 Class 1 - 1.Internal actors(Difi)

This class represents all the internal actors that are somehow connected to MinID, either through employment or other means. These actors include the Difi management, Difi departments, developers, operators, and generally all who has a stake in the project.
Difi developed the solution called MinID, and operates the IdMS on a day to day basis. Difi is funded by the government, and we make the assumption that it is a non-profit organization. As a basis for this stakeholder analysis, some assumptions (unconfirmed) have been made about their

performance indicators:

- Number of people using MinID (compared to other eID providers).
- Availability of MinID.
- Integrity and confidentiality of service.
- Customer satisfaction.
- Available sites and services.
- Contributions to the Public Services (ease of access, digitalization of services, knowledge).

Difi answers to the Ministry of Government Administration, Reform and Church Affairs (FAD), referred to as *Government* (see section C.3.2) in this analysis, which also controls funding for further project work in Difi. Difi has one management department which is considered as a single stakeholder in this analysis. Difi also has seven sub departments [74], three of these departments have been grouped into one stakeholder ,Difi Departments, while the last four are regarded as trivial for project, and is therefore not a part of the stakeholder analysis. The last stakeholder in Difi is internal threat agents, this group is represented by the malicious insiders and the non-compliant employee.

Class 2 - 1.Difi Management

Difi Management are decision makers, both for Difi as an organization and for the MinID system. This stakeholder consists of the CEO, assistant director and staff (communications unit (KEN)). The group has been rated has highly influential in the project since they are in charge of Difi, and they have been given high importance, this is because they have a share of the responsibility for the project, as well as a stake in the project lifetime. The incentives of the Difi Management are political (i.e. gaining more funding through political support), financial (obtain more funding), business and self assertion (i.e. promoting one self for promotions). They have a positive attitude towards the project, as some of their reputation depend on it.

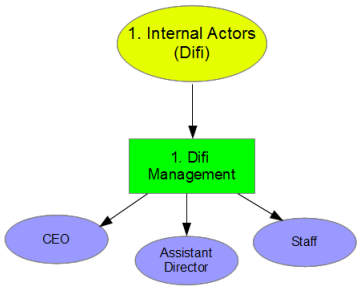


Figure 48: Stakeholder branch 1.1

Table 1: Difi Management Attributes

Influence	Importance	Incentives	Attitude	Allies	Opponents
High	High	Political	Positive	Difi Departments	Int threats
		Financial		Users	Competitors
		Business			Ext. attackers
		Self assertion			

Class 2 - 2.Difi Departments

May also be referred to in the stakeholder analysis as Difi ICT. These are the departments that have been found to be significant, and have a direct stake and influence in the project. This stakeholder grouping consists of three departments which have been found to have a direct stake in MinID, ICT development and governance (UFI), ICT management and coordination (ITS) and governance and organization (FOR). The ICT departments (UFI and ITS) were included because of their involvement in MinID development and operations, and FOR is included because they were policy makers. These departments need to have political support for the MinID solution, to be able to sustain their jobs and funding. They are also interested in sustaining/increasing the number of users for the system through strengthening of business processes and more funding. Both their influence and importance to the project has been rated as high and they have a positive attitude towards the project, because MinID is a part of their job.

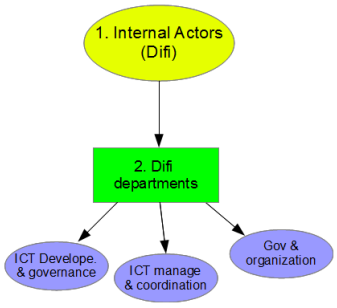


Figure 49: Stakeholder branch 1.2

Table 2: Difi Departments Attributes

Influence	Importance	Incentives	Attitude	Allies	Opponents
High	High	Political	Positive	Difi management	Int threats
		Financial		Regulatory Services	Competitors
		Business			Ext. attackers

Class 2 - 3.Internal threat agents

This class consists of the malicious insider and the non-compliant employee, and represent the human factor in information security. The non-compliant employee is the employee that has no malicious intent, but endanger the organization through breaches of security routines and/or policy. The non-compliant employee may also be referred to as the inadvertent insider.
The malicious insider is a threat that may exists within organizations, they can i.e. destroy information, sell sensitive business/system information and cause havoc. This threat class has the potential of causing extensive damage due to their inside knowledge of the system.

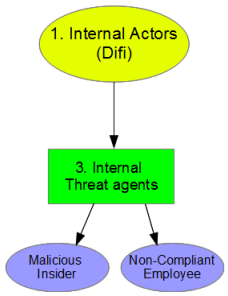


Figure 50: Stakeholder branch 1.3

This class has a low influence in the project because this is likely to be the common employee (but it is also possible for decision makers to be a malicious insider). They have been given high importance because of their capability of causing harm to the system. This stakeholder is negative for the MinID project. They may be motivated by financial gain, terrorism (destruction), grudging (revenge), fun or just carelessness.

Table 3: 1.3 Internal Threat Agents Attributes

Influence	Importance	Incentives	Attitude	Allies	Opponents
Low	High	Political	Negative	Ext. Attackers	Difi departments
		Financial			ID-portal
		Terrorism			Users
		Grudging			Difi Management
		Fun			Regulatory Services
		Carelessness			

C.3.2 Class 1 - 2. Government

This class represents government stakeholders that have interaction with MinID. Difi answers to the Ministry of Government Administration, Reform and Church Affairs (FAD), and receives funding from this instance.

Class 2 - 1.Regulatory services

The government bodies included in this class have a stake in MinID. These are the Norwegian Data Inspectorate, Privacy committee (Personvernnemda) and policy, law and legislation makers. All these are grouped into one stakeholder called "Regulatory services". This is a highly influential stakeholder which is in charge of funding and auditing, they were also involved in creating the requirements for the public key infrastructure in Norway. Their importance to the project is also high due to that Difi must prove that MinID is a viable solution to the government for future existence. Their attitude towards the project is positive, as these represent one of the initiating factors for the MinID project. They also possess knowledge of their ability to force changes in MinID through new policies, laws and legislations. They are positive to the project, and as they have helped develop the requirements, they have a stake in how well the system performs.

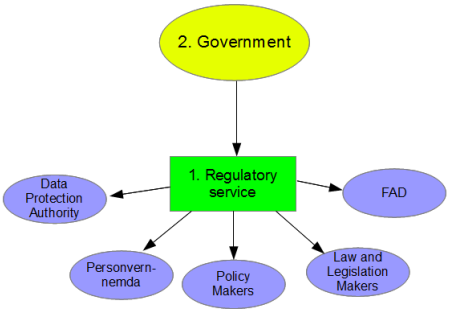


Figure 51: Stakeholder branch 2.1

Table 4: 2.1 Regulatory Services Attributes

Influence	Importance	Incentives	Attitude	Allies	Opponents
High	High	Political	Positive	Difi Departments	Int threats
		Financial		Difi Management	Ext. attackers
		Business		Users	
				ID-portal	

C.3.3 Class 1 - 3. External users

This class represents users of the MinID IdMS, which are mainly Norwegian citizens and holders of D-numbers, and Norwegian municipalities and departments. Since this case is concerned with privacy risks, we chose to disregard the latter as they had little consequence regarding privacy and focus on the users.

Class 2 - 1.Users

This stakeholder group consists of Norwegian citizens and holders of D-numbers. The users are the main target group for the MinID project, and the system is scoped and developed to fit the users requirements, they are therefore given high importance. Even though the system is scoped for the users, they have low influence in MinID. The IdMS facilitates electronic access to governmental services, and users have a stake in the availability and functionality of the system. The users are positive towards the MinID project, because it allows for ease-of-access. The users can use MinID for political means (eVote), and for financial purposes (Tax). The data in the MinID database may impact the users business if it becomes public.

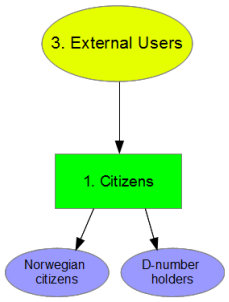


Figure 52: Stakeholder branch 3.1

Table 5: 3.1 Users Attributes

Influence	Importance	Incentives	Attitude	Allies	Opponents
Low	High	Political	Positive	Regulatory Services	Int threats
		Financial			Ext attackers
		Business			

C.3.4 Class 1 - 4. Service Providers

This class represents the other service providers that can be used to access the ID-portal, and the available public services available through the ID-portal. The scope of this case can be seen in figure 24, although these services are outside of the scope, they are still important stakeholders that need consideration. All of the services provided by the government and available through the ID-portal has been classified at as the group "ID-portal", and the other eID providers have been classified as "Competitors".

Class 2 - 1. Competitors

This stakeholder represents all other eID providers in the ID-portal. The assets and the capabilities of this stakeholder has been scoped down to only that which is related to privacy. The competitors are mainly focused on financial aspects, such as making money and gaining financial advantages to strengthen business processes and attract more users. This analysis does not consider threats to competitors, such as attackers.

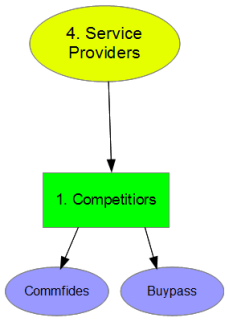


Figure 53: Stakeholder branch 4.1

This stakeholder has low importance on the MinID project, since the competition does not require any considerations for implementing and operating MinID. But they have medium influence because solutions produced by competition that improves their IdMS can result in MinID, either adapting these solutions for their own or risk losing revenue. This stakeholder is a competitor to the MinID project, and is therefore negative towards the project.

Table 6: 4.1 Competitor Attributes

Influence	Importance	Incentives	Attitude	Allies	Opponents
Medium	Low	Financial	Negative		Difi Departments
		Business			Difi Management

Class 2 - 2. ID-portal

The ID-portal stakeholder represents all the service providers accessible through MinID. Some of these services handle sensitive personal information for each user, but this data handling is not within the scope of this case. This stakeholder can influence changes, but they do not represent a legislature authority and therefore have medium influence on the MinID project. Major considerations must be given to this stakeholder when designing MinID and therefore have high importance. They have political incentives in that they may wish to obtain more funding through politics, and a privacy related incident will affect them negatively, and have them loose political support. They also have a business incentive, as have a solution that is measured in amount of visits, more users will raise arguments for more funding.

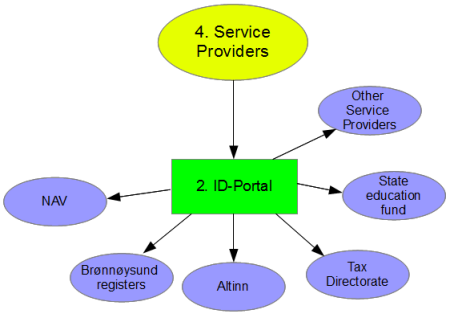


Figure 54: Stakeholder branch 4.2

This stakeholder is neutral regarding MinID as it is unlikely that they care which solution the users apply to access their systems.

Table 7: 4.2 ID-portal Attributes

Influence	Importance	Incentives	Attitude	Allies	Opponents
Medium	High	Political	Neutral	Regulatory Services	Int threats
		Business			Ext attackers

C.3.5 Class 5 - 1. External threats

This class represents external threats to the system, these have been identified as (but not limited to) hackers, crackers, computer criminals, terrorists, industrial spies and automated attacks (such as worms, virus and other malware).

Class 2 - 1. Attackers

This stakeholder group has a passive influence on the project. Based on the capabilities of the attackers, the applications must be secured in such a way that the attacker does not gain access to the system, this stakeholder therefore has a medium influence. MinID handle personal data and they must secure this information as specified by law to prevent unauthorized access to this data. Unauthorized data accesses is mainly caused by this stakeholder group, and therefore has high importance in the MinID project.

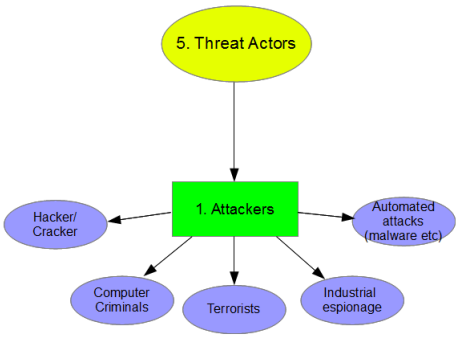


Figure 55: Stakeholder branch 5.1

The stakeholder has a negative attitude towards the project, and is a threat actor that is likely to cause harm to the MinID system if given the chance. Their incentives are mainly financial (personal gain), but may also include political purposes (such as stealing and revealing information to cause political harm and gain advantage), obtain business advantage, hack for terrorism or self assertion, grudging (revenge), fun (i.e. to see if the attacker is able to break the system), or to gather intelligence for the military. This stakeholder has a high knowledge of their own capabilities and are aware that their opponents know of their existence.

Table 8: 5.1 Attacker Attributes

Influence	Importance	Incentives	Attitude	Allies	Opponents
Medium	High	Political	Negative	Int threats	Difi Departments
		Business			ID-portal
		Financial			Users
		Terrorism			Difi Management
		Grudging			Regulatory services
		Self assertion			
		Fun			
		Military			

C.4 Summary of the Scenario description

The first part of the scenario addresses the background and objectives of MinID, why it was developed, and by whom. The most important laws and regulations that Difi is subject to has been addressed, together with the existing MinID privacy policies. Difi is regarded as a data handler according to Norwegian law, but is only responsible for the personal information within their system. They are not responsible for the information accessed using MinID. "Two" databases are used by MinID, one that stores personal data about the users, such as birthnumber, and a high level database that stores sensitive personal data about the users, i.e. log in IP addresses, and time and date for logins.

To limit the number of identified stakeholders, the limit of class three stakeholders was set to eight. This was done to limit the complexity and time use of the task. All the stakeholder classes have either significant influence or importance in the MinID project, with emphasis on capabilities and assets concerning personal data. The presentation of the stakeholders in this chapter is a summary of the complete stakeholder analysis found in appendix D.

D Appendix - Stakeholder Analysis

Stakeholder Analysis for Identity Management Systems (Case study: MinID by Difi)

by
Gaute Wangen, Master Information security
Gjøvik University College 2012

Introduction to this document

This document was written as documentation for the master's thesis "Risk Analysis for Privacy and Identity Management". It first presents the template used for the stakeholder analysis in the thesis, with short explanations of each stakeholder attribute (for a more detailed description and explanation of the attributes in the template, see chapter 3 – Methodology in the thesis). The eight full stakeholder analysis produced for the thesis are then presented.
(For an example of how to use this stakeholder analysis see the thesis.)

Table of contents:

Stakeholder analysis template v1.5

Category 1.2.3:

1. Influence and importance in project: (*Influence vertical and importance horizontally)*
High – Medium - Low
i.e. Influence vertical and importance horizontally

2. Capabilities:
What actions can the stakeholder perform?
Examples of capabilities for stakeholders:
- Influence project decision
- Stop funding
- Increase funding
- Shut down project
- Register
- Log in
- Read, write, delete, alter database information
- Copy – datamine database information
- Steal/Sell personal information
- Attack – DoS, worm, virus, etc

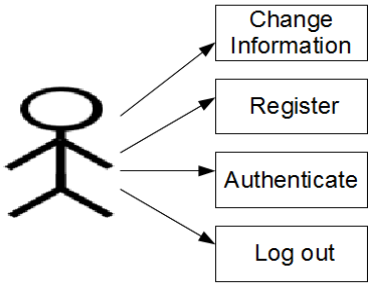


Illustration 1: Example of capability illustration

3. Incentive matrix:
List of suggestions for incentives for actors: military, political, business, financial, advertisement, terrorism, grudging, self assertion, fun, carelessness. These incentives can be used in evaluation of assets.

Political		Gruding	
Financial		Self assertion	
Business		Fun	
Advertisement		Military	
Terrorism		Carelessness	

4. Attitude and knowledge of the project

Attitude signifies positivity(+), neutrality (0), negativity (-) towards the project.
Knowledge level, three levels of knowledge, 1 is lowest, 3 is highest. Attitude, knowledge and asset evaluation can be used to calculate likelyhood of a stakeholder acting on a capability.

ATTITUDE (+/0/-)	REASONING	KNOWLEDGE (1/2/3)	REASONING

5. Stakeholder assets:

Asset is something that is of value to somebody, A valuable entity. This method suggest dividing intagible assets and tangible assets into two tables.
The example tables contains suggestions for possible assets that may be used in the project.

INTANGIBLE ASSETS		
ASSET	ESTIMATED VALUE FOR STAKEHOLDER	REASONING
Subscriber Privacy		
MinID Database information		
User Sensitive Personal information		
User logs		
User login data		
Computer Software		
Computerized Databases		
TANGIBLE ASSETS		
ASSET	ESTIMATED UTILITY VALUE	REASONING
Funding		
Cash		

6. Relationship with other stakeholders

The allies of each stakeholder is used to determine who they want to affect positively or negatively.

ALLIES	NEUTRAL	OPPONENTS

7. Consequences of capabilities on assets and affected stakeholders:

When analysing capabilities, how does:
- the actions of the stakeholder impact the assets?
- change relations with other stakeholders?
- change value of assets?

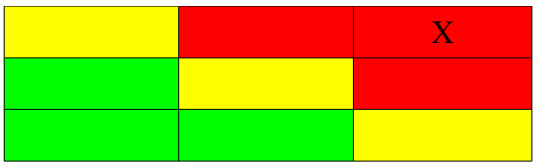
Does the capability create points of tension where privacy comes under pressure?
- does the affected stakeholder care? -> evaluation of assets

CAPABILITY	ASSET(s) AFFECTED (Positive or negative)	EFFECT *(for stakeholder)*	AFFECTED STAKEHOLDERS (Positive or negative)

Difi Management Analysis

1. Internal Actors – 1. Difi Management – CEO, Assistant Director, Staff

Influence and importance in project: (*Influence vertical and importance horizontally)*



Difi Management have high influence of the project, given that they are in charge of the Difi. They are given high importance, as they have a share of the responsibility for the project, and its lifetime.

Capabilities:

- Create/Enforce new Security policy
- Administer funding to new security measures
- Evaluate security
- Retain funding from security measures
- Increase funding to other measures
- Enforce compliance to laws and regulations
- Shut down project

Incentive matrix:

Political	X	Gruding	
Financial	X	Self assertion	X
Business	X	Fun	
Advertisement		Military	
Terrorism		Carelessness	

Attitude towards and knowledge of the project

Attitude signifies positivity(+), neutrality (0), negativity (-) towards the project. Good/bad actor. Knowledge level, three levels of knowledge, 1 is lowest, 3 is highest.

ATTITUDE (+/0/-)	REASONING	KNOWLEDGE (1/2/3)	REASONING
+	They have part of the responsibility for the project, and are likely to want to see it succeed.	3	Management knows of their capabilities.

Stakeholder assets:

INTANGIBLE ASSETS		
ASSET	ESTIMATED VALUE FOR STAKEHOLDER	REASONING
Security Policies	Medium	May impact business
Revenue (MinID Subscribers)	High	Business and financial.
CIA of MinID services	Medium	May impact business and financial
Goodwill	Medium	May impact business, political and self-assertion
System Security	Medium	May impact business and financial
Usability	Medium	May impact business and financial
Subscriber Privacy	Medium	May impact business, political and financial
Reputation	High	Financial, business, political and self-assertion
TANGIBLE ASSETS		
Internal funds	High	Financial, business and political

Relationship with other stakeholders

ALLIES	NEUTRAL	OPPONENTS
Difi departments	ID-portal	Internal threat agents
Regulatory services	Citizens (Users)	Competitors
		Ext. Attackers

Consequences of capabilities on assets:

CAPABILITY	ASSET(s) AFFECTED (Positive or negative)	EFFECT *(for stakeholder)*	AFFECTED STAKEHOLDERS (Positive or negative)
- Create/Enforce New Security Policy - Administer funding to new security measures - Evaluate and improve existing security measures	- System Security (+) - Security Policies (+) - Internal funds (-) - Revenue (0) - Usability (-) - Subscriber Privacy (+)	- Increase in system security decreases chance for security incident. - Decreases funding for improvement/addition of other services. - Decreased Usability for the *User.* - Improved security for *Users.* - Improved privacy for *Users.* - Decreased need for Government interaction with Difi.	- Difi ICT (+) - Internal threat agents (-) - Regulatory Servicest (+) - External threats (-)
- Retain funding from security measures - Increase funding on other measures	- System Security (-) - Security Policies (-) - Internal funds (+) - Revenue (+) - Subscriber Privacy (-)	- Free up funding for other projects within Difi or MinID, which can increase revenue and improve usability for the *Users.* - But reduce privacy for *Users*	- Internal threat agents (+) - External threats (+) - Users (-)
- Ensure compliance, laws, regulations and government policy	- System security (+) - Subscriber privacy (+) - Reputation (+) - Internal funds (+) - Revenue (+)	- Following government guidelines increases security and lifts the reputation of the organisation. - As long as the project abides by the guidelines and obtains more users while keeping the old ones.	- Government (+) - Difi ICT (+) - Internal threat agents (-) - External threats (-) - Competition (-) - Users (+)

Difi Departments Analysis

1. Internal actors (Difi) – 2. Difi Departments – ICT dep, Governance and Organization dep.

Influence and importance in project: (*Influence vertical and importance horizontally)*

This stakeholder include developers of the system, and therefore have a *high* influence on the project. This group also includes the operators and front line communication with the customers of the system, and therefore have a *high* importance in the system.

Capabilities:
- Access MinID database (Read) – i.e. Customer service
- Write to database information (Write) – i.e. Customer service
- Enforce security
- Create/Enforce Policy
- Create/Enforce Security Functionlity
- Access to high level logs (Read\write)
- Merge login – times – IP – which site the user visited (to help prevent fraud and abuse)

Incentive matrix:

Political	X	Gruding	
Financial	X	Self assertion	
Business	X	Fun	
Advertisement		Military	
Terrorism		Carelessness	

Attitude towards and knowledge of the project

Attitude signifies positivity(+), neutrality (0), negativity (-) towards the project. Good/bad actor. Knowledge level, three levels of knowledge, 1 is lowest, 3 is highest.

ATTITUDE (+/0/-)	REASONING	KNOWLEDGE (1/2/3)	REASONING
+	These departments are responsible for MinID operations and stability. Their job security depend on them keeping MinID stable and attractive to customers	3	These departments were responsible for designing and implementing MinID, and know of their capabilities within MinID

Stakeholder assets:

INTANGIBLE ASSETS		
ASSET	ESTIMATED VALUE FOR STAKEHOLDER	REASONING
MinID Database information	High	Business, political and financial
MinID User logs	High	Business, political and financial
Subscriber privacy	High	Business, political and financial
Usability	Medium	May impact Business
System security (firewall settings, IDS, etc)	High	Business
Security policies	Medium	May impact political and business
Revenue (MinID Subscribers)	High	Business
Goodwill	Medium	Political and Financial
TANGIBLE ASSETS		
Funds	High	Business and Financial

Relationship with other stakeholders

ALLIES	NEUTRAL	OPPONENTS
Difi management	ID-portal	Internal threat agents
Regulatory services	Citizens (Users)	Competitors
		Ext. Attackers

Consequences of capabilities on assets:

CAPABILITY	ASSET(s) AFFECTED (Positive or negative)	EFFECT *(for stakeholder)*	AFFECTED STAKEHOLDERS (Positive or negative)
Customer service: - Access MinID database (Read) - Write to database information (Write)	- Subscriber privacy (-) - Goodwill (+) - Revenue (+)	- *User* increases in satisfaction, a reduction in privacy, ease of access on personal data. - Increase in Goodwill, which may implicate more revenue gains Difi management - Gains External attacker, opens potential attack path (Phone phreaking) - Eases access for the *Internal threat agents* - *Regulatory services* may object.	- Users (-) - Difi management (+) - External Attacker (+) - Internal threat agents (+) - Competition (-) - Regulatory services (-)
- Enforce security - Create/Enforce Policy - Create/Enforce Security Functionlity	- System Security (+) - Security Policies (+) - Funds (-) - Usability (-) - Subscriber Privacy (+)	- Increase in security helps *privacy* - Funds are redused as money is spent on security measures and not other alternatives - Usability is reduced because of increase security.	- User (+) - External Threat Actors (-) - Internal threat agents (-)
- Access to high level logs (Read\write) - Merge high level logs	- System security (+) - Subscriber privacy (-) - MinID DB information (+)	- Increase in system integrity and security, as merging of logs can help detect anomalies in the system. - Privacy issues for the *Users* regarding logs. - *Internal threat agents* gets access to more sensitive information, when database increase in value. - Opens possibility for cross referencing sites the user accessed at which times.	- User (-) - Internal threat agents (+)

Malicious insider and Non-Compliant Employee

5. Internal Actors - 3. Internal Threat Agents - Malicious Insider and Non-compliant Employee

Influence and importance in project: (*Influence vertical and importance horizontally)*

The malicious insider has the influence of the common employee, and can only suggest changes to the system, which gives this stakeholder a *low* influence.
The stakeholder has the capability of causing great harm to the system, and should be considered as a major threat, and is therefore given *high* importance.

Capabilities:

- Access MinID database (Read)
- Corrupt database information (Write)
- Delete database information (Delete)
- Datamine/gathering
- Steal/Sell personal information
- Attack – DoS, worm, virus, etc
- Steal credentials - Massquerade
- Steal/Sell system documentation
- Espionage

Incentives:

Political	X	Gruding	X
Financial	X	Self assertion	
Business		Fun	X
Advertisement		Military	
Terrorism	X	Carelessness	X

Attitude towards and knowledge of the project

ATTITUDE (+/0/-)	REASONING	KNOWLEDGE (1/2/3)	REASONING
-	This stakeholder group can cause harm intentionally or unintentionally.	3	The malicious insider is likely to be very knowledgeable about the system and his own capabilities. While the the non-compliant employee, may not be aware of the consequences of his/hers actions.

Stakeholder assets:

INTANGIBLE ASSETS		
ASSET	ESTIMATED VALUE FOR STAKEHOLDER	REASONING
Anonymity	High	Financial, Political
Freedom	High	Financial, Political
System damage	High	Financial, Gruding, Fun, Carelessness, Terrorism, Political
MinID Database information	Low	Financial, Political, Grudging, Fun, Carelessness
Subscriber privacy	Low	Financial
System documentation (security information, trade secrets)	Low	Financial, Gruding, Fun, Carelessness, Terrorism, Political
TANGIBLE ASSETS		
Cash	High	Financial

Relationship with other stakeholders

ALLIES	NEUTRAL	OPPONENTS
Ext. Attackers	Competitors	Difi departments
		ID-portal
		Citizens
		Difi Management
		Regulatory services

Consequences of capabilities on assets:

CAPABILITY	ASSET(s) AFFECTED (Positive or negative)	EFFECT *(for stakeholder)*	AFFECTED STAKEHOLDERS (Positive or negative)
Read/Copy Datamining Masquerade Espionage Selling information	- Cash (+) - MinID database (-) - System Documentation (-) - Subscriber privacy (-) - Anonymity (-)	- Obtain information about *User(s)* and *Internal actors (Difi)* - Lose Anonymity by doing a malicious action. - Gain cash by selling information to competitors or Ext attackers - All system related information looses value once it is public.	- User (-) - Difi Management (-) - Difi ICT (-) - Competitors (+) - Ext Attackers (+)
Corrupt or Delete	- System damage (+) - MinID database (-) - System Documentation (-) - Subscriber privacy (-) - Anonymity (-)	- Corruption/removal of data from *Internal actors (Difi)* causing loss of availablity - *Internal actors* loose revenue	- User (-) - Difi Management (-) - Difi ICT (-) - Competition (+)
Attack	- System damage (+) - MinID database (-) - System Documentation (-) - Subscriber privacy (-) - Anonymity (-) - Freedom (-)	- Disrupt availability for *User(s), Internal actors (Difi), Service Providers.* - *Internal actors* loose revenue - Attacker may publish privacy related information - Attacker risks Anonymity and Freedom	- User (-) - Difi Management (-) - Difi ICT (-) - Competition (+)

Government Regulatory services

2. Government – 1. Regulatory services – Data protection authority, Personvernnemda, etc...

Influence and importance in project: (*Influence vertical and importance horizontally)*

The government has *high* influence, as they can shut down the project or increase/decrease funding for major effect. It has *high* importance in the project, as Difi must prove that MinID is a viable solution for it to continue existing, giving the government direct importance for continued survival of the project.

Capabilities:

- Increase / decrease funding
- Stop funding
- Shutdown project
- Penalize Difi
- Ensure compliance
- Create policy
- Create Laws
- Create Regulations
- Audit (triggered by User complaints)
- Enforce policy, laws, regulations

Incentive matrix:

Political	X	Gruding	
Financial	X	Self assertion	
Business	X	Fun	
Advertisement		Military	
Terrorism		Carelessness	

Attitude towards and knowledge of the project

Attitude signifies positivity(+), neutrality (0), negativity (-) towards the project. Good/bad actor. Knowledge level, three levels of knowledge, 1 is lowest, 3 is highest.

ATTITUDE (+/0/-)	REASONING	KNOWLEDGE (1/2/3)	REASONING
+	Initiators of the project, controls funding.	2	Knows of their own capabilities and influence on the MinID project. But may not be aware of the implications of actions regarding privacy.

Stakeholder assets:

INTANGIBLE ASSETS		
ASSET	ESTIMATED VALUE FOR STAKEHOLDER	REASONING
Goodwill	Medium	May impact political and business
Revenue (MinID Subscribers)	Medium	May impact financial and business
Laws, Regulations, Policies	High	Business, Financial, Political
Reputation	Medium	May impact political, financial and business
Subscriber Privacy	High	Business (Data protection authority)
TANGIBLE ASSETS		
Funds	High	Financial

Relationship with other stakeholders

ALLIES	NEUTRAL	OPPONENTS
Difi departments	Competitors	Internal threat agents
Difi Management		Ext. Attackers
Citizens (Users)		
ID-portal		

Consequences of capabilities on assets:

CAPABILITY	ASSET(s) AFFECTED (Positive or negative)	EFFECT *(for stakeholder)*	AFFECTED STAKEHOLDERS (Positive or negative)
- Increase funding	- Funds (-) - Goodwill (+) - Revenue (+) - Subscriber Privacy (+)	- Increase funding for *Difi*, gives more possibilities for increasing revenue. - Strengthens relationship between departments through Goodwill. - May increase *User* privacy	- Difi Management (+) - Difi ICT (+) - Users (+) - Competition (-)
- Decrease funding - Penalize Difi - Shutdown project	- Funds (+) - Goodwill (-) - Reputation (-) - Subscriber privacy (-)	- Funds increase due to decrease in Difi funding, penalties or shutdown. - Goodwill is reduced due to less funding. - Loss of Reputation can occur given that the government has a direct stake in the MinID solution.	- Difi Management (-) - Difi ICT (-) - Competition (+) - Users (-)
- Influence project development - Create policy - Create Laws - Create Regulations	- Laws, regulations, Policies (+) - Subscriber Privacy (+) - Goodwill (-)	- More laws, regulations and policies increase security and privacy. - Forcing more laws, regulations, policies causes loss of goodwill from *Internal Actors*.	- Users (+) - Difi Management (-) - Difi ICT (-) - Internal threat agents (-) - External threats (-)
- Audit - Enforce policy, laws, regulations	- Funds (-) - Goodwill (-) - Reputation (-) - Subscriber Privacy (+)	- Triggered through complaints to *Complaint handlers*, this decreases funds which is used on auditing *Difi and MinID*. Goodwill and Reputation is at stake if the auditors find irregularities. - Privacy and security increases for the *Users* because of system auditing.	- Users (+) - Difi Management (-) - Difi ICT (-) - Internal threat agents (-) - External threats (-)

User, Norwegian citizens and D-number holders

3. External users – 1. Citizens - Users

Influence and importance in project: (*Influence vertical and importance horizontally*)

The Users can not directly influence the system given that the system is developed by the the government and has *low* influence. The Users have *high* importance in this system, as it is a single sign on system developed for all the Norwegian citizens.

Capabilities:

- Register
- Unregister
- Log in/out (authenticate)
- Use services in ID-Portal
- Change personal information
- Change password
- Order PIN codes
- Register complaint

Incentive matrix:

Political	(X)	Gruding	
Financial	X	Self assertion	
Business	X	Fun	
Advertisement		Military	
Terrorism		Carelessness	

Attitude towards and knowledge of the project

ATTITUDE (+/0/-)	REASONING	KNOWLEDGE (1/2/3)	REASONING
+	User has a personal stake in MinID. Changes in the system will have immediate consequences for the user. System facilities access to governmental services.	2	The capabilities of the user are well documented and made available for the user. But may not be aware of privacy implications.

Stakeholder assets:

INTANGIBLE ASSETS		
ASSET	ESTIMATED VALUE FOR STAKEHOLDER	REASONING
Privacy	High	Financial, business, political
MinID Database (including logs)	Low	May impact financial, business, political
Availability (of services)	High	Financial, business, political
TANGIBLE ASSETS		
-		

Relationship with other stakeholders

ALLIES	NEUTRAL	OPPONENTS
Regulatory services	ID-portal	Internal threat agents
	Competitors	Ext. Attackers
	Difi departments	
	Difi Management	

Consequences of capabilities on assets:

CAPABILITY	ASSET(s) AFFECTED (Positive or negative)	EFFECT *(for stakeholder)*	AFFECTED STAKEHOLDERS (Positive or negative)
- Register	- MinID database (+) - Privacy (-) - Availability (+)	- User is registered in the *Difi* database for users - Registers personal information with a third party, decreasing privacy. - Makes information available for internal threat agents.	- Difi Management (+) - Difi ICT (+) - ID-Portal (+) - Regulatory Services (+) - Internal threat agents (+) - Competitors (-)
- Unregister	- MinID database (-) - Privacy (+) - Availability (-)	- User unregisteres from the *Difi* database for users, and removes personal information from third party.	- Difi Management (-) - Difi ICT (-) - Internal threat agents (-) - ID-Portal (-) - Government (-)
- Log in/out (authenticate) - Use services in ID-Portal - Order PIN codes - Change personal information	- MinID database (+) - Availability (+) - Privacy (-)	- The logs in MinID database increase in information and gain value. - Increase in logs puts privacy of the user is in jeopardy. - Number of log ins gains Internal actors	- Difi Management (+) - Difi ICT (+) - Internal threat agents (+) - Regulatory Services (+)
- Register complaint	- Privacy (+)	- User registers complaint about MinID, with the *Governmentally* owned *Personvernnemda,* which is force to take action. - Privacy increases as an effect of i.e. external audits.	- Internal actors (-) - Regulatory Services (-) - Competition (+)

Competitors

4. Service providers – 1. Competitors

Influence and importance in project:

The competition is judged to have *medium* influence in the MinID project. this is because improving solutions produced by competition will result in MinID, either adapting these solutions for their own or risk losing revenue.
Stakeholder has *low* importance, since the competition does not require any considerations for implementing and operating MinID.

Capabilities:
- Influence users
- Log login – times – IP – which site the user visited
- merge logs

Incentive matrix:

Political		Gruding	
Financial	X	Self assertion	
Business	X	Fun	
Advertisement		Military	
Terrorism		Carelessness	

Attitude towards and knowledge of the project

Attitude signifies positivity(+), neutrality (0), negativity (-) towards the project. Good/bad actor. Knowledge level, three levels of knowledge, 1 is lowest, 3 is highest.

ATTITUDE (+/0/-)	REASONING	KNOWLEDGE (1/2/3)	REASONING
-	The competitors have their customers from the same exhaustive user mass that MinID has. A bigger share of the user mass means more money.	3	Knows about their capabilities in obtaining more users, and are also knowledgeable about privacy risks.

Stakeholder assets:

INTANGIBLE ASSETS		
ASSET	ESTIMATED VALUE FOR STAKEHOLDER	REASONING
Database information	Medium	May impact financial and business
User logs	Medium	May impact financial and business
Revenue	High	Financial, Business
Subscriber Privacy	Medium	May impact financial and business
Security	High	Financial, Business
TANGIBLE ASSETS		
Funds	High	Financial

Relationship with other stakeholders

ALLIES	NEUTRAL	OPPONENTS
	ID-portal	Difi departments
	Internal threat agents	Difi Management
	Ext. Attackers	
	Citizens	
	Regulatory Services	

Consequences of capabilities on assets:

CAPABILITY	ASSET(s) AFFECTED (Positive or negative)	EFFECT *(for stakeholder)*	AFFECTED STAKEHOLDERS (Positive or negative)
- Influence users - Innovate/implement new functionalities	- Funds (-) - Revenue (+) - Subscriber privacy (-) - Database information (+)	- More investments in influencing users and improving software attracts more users, but drains funds. - User shares personal data with another actor	- Difi Management (-) - Difi ICT (-) - Internal threat agents (-) - Users (-) - Regulatory Services (-)
- Log userinfo - merge logs	- Subscriber privacy (-) - Database information (+) - User logs (+) - Security (+)	- Privacy issues for the *Users* regarding logs. - Opens possibility for cross referencing sites the user accessed at which times.	- User (-)

ID-Portal

4. Service Providers – 2. ID-portal – Norwegian tax administration, telephone company, NAV, etc...

Influence and importance in project: (*Influence vertical and importance horizontally)*

This stakeholder is the group for which MinID is a SSO, and therefore can influence changes in MinID. But they do not represent a legislature authority, and therefore are labeled *medium* influence. Major considerations must be given to this stakeholder when designing MinID, *high* importance.

Capabilities:
- Provide personal data for eID providers
- generate PIN-codes
- send pin-letter
- send PIN sms

Incentive matrix:

Political	X	Gruding	
Financial		Self assertion	
Business	X	Fun	
Advertisement		Military	
Terrorism		Carelessness	

Attitude towards and knowledge of the project

Attitude signifies positivity(+), neutrality (0), negativity (-) towards the project. Good/bad actor. Knowledge level, three levels of knowledge, 1 is lowest, 3 is highest.

ATTITUDE (+/0/-)	REASONING	KNOWLEDGE (1/2/3)	REASONING
0	Of the three identity providers that provide access to the ID-portal, we do not know of any reasons why this group should favor one of the identity providers over the other	1	May not be aware of their influence on the project.

Stakeholder assets:

INTANGIBLE ASSETS		
ASSET	ESTIMATED VALUE FOR STAKEHOLDER	REASONING
Personal data	Medium	May impact political, business
Subscriber Privacy	High	Political, business
PIN codes	Low	No probable impact
Sensitive personal data	High	Political, business
Goodwill	High	Political, business
Reputation	High	Political, business
TANGIBLE ASSETS		
-		

Relationship with other stakeholders

ALLIES	NEUTRAL	OPPONENTS
Regulatory Services	Competitors	Internal threat agents
	Difi departments	Ext. Attackers
	Difi Management	
	Citizens	

Consequences of capabilities on assets:

CAPABILITY	ASSET(s) AFFECTED (Positive or negative)	EFFECT *(for stakeholder)*	AFFECTED STAKEHOLDERS (Positive or negative)
- Provide personal data for eID providers	- Personal data (-) - Subscriber privacy (-) - Goodwill (+)	- Personal data is shared with MinID (or other eID provider). - Privacy is weakened for the *Users* through sharing of personal data.	- Users (-) - Difi Management (+) - Difi ICT (+) - Internal threat agents (+)
- Genereate PIN-codes - Send PIN-letter - Send PIN- SMS	- Pin codes (+) - Goodwill (+) - Subscriber Privacy (-)	- Stakeholder uses third party to distribute PIN codes to *Users.* - Privacy is weakened since third party obtains knowledge about the *Users* registering with MinID - Security is strengthened through two factor auhentication.	- Users (-) - Difi Management (+) - Difi ICT (+) - Regulatory Services (+)

External Attackers

5. External Threats – 1. Attackers – Hackers/crackers, Computer criminals, terrorist, industrial spies, automated attacks.

Influence and importance in project:

This stakeholder group has a passive influence on the project, the applications must be secured in such a way that this stakeholder does not gain access to the system, *medium* influence. As MinID handles personal information, they must secure this information as specified by law to prevent unauthorized access to this information, *High* importance.

Capabilities:

- Automated attacks (ddos, vandalism, worms, etc)
- Targeted attacks (Phising, e-mail with malware, etc)
- Buy personal data
- Hack accounts
- Register new user with unregistered birthnumbers (in Difi DB)

Incentive matrix:

Political	X	Gruding	X
Financial	X	Self assertion	X
Business	X	Fun	X
Advertisement		Military	X
Terrorism	X	Carelessness	

Attitude towards and knowledge of the project

Attitude signifies positivity(+), neutrality (0), negativity (-) towards the project. Good/bad actor. Knowledge level, three levels of knowledge, 1 is lowest, 3 is highest.

ATTITUDE (+/0/-)	REASONING	KNOWLEDGE (1/2/3)	REASONING
-	This is external threat actors which want to cause harm to the system or obtain confidential information	2	This stakeholder group is aware of its own capatilities and alternatives for causing harm and penetrating the system. They are also aware that their opponents know of their existence, but does not know capabilities of opponents

Stakeholder assets:

INTANGIBLE ASSETS		
ASSET	ESTIMATED VALUE FOR STAKEHOLDER	REASONING
Anonymity	High	Fun, Political, Financial, Self assertion
Freedom	High	Financial, Business, Fun
System damage	High	Financial, Gruding, Fun, Carelessness, Terrorism, Political
Personal data (MinID DB)	High	Political, financial, business, gruding, fun, military, self assertion
Sensitive personal data (MinID DB logs)	High	Political, financial, business, gruding, fun, terrorism, military, self assertion
System documentation (Security settings, etc)	High	Financial, gruding, fun, terrorism, military, business, self assertion
Birth numbers	Medium	May impact Financial, Self assertion, Fun.
Subscriber privacy	None	Does not value privacy of subscribers
TANGIBLE ASSETS		
Cash	High	Financial

Relationship with other stakeholders

ALLIES	NEUTRAL	OPPONENTS
Internal Threat Agents	Competitors	Difi departments
		ID-portal
		Citizens
		Difi Management
		Regulatory services

Consequences of capabilities on assets:

CAPABILITY	ASSET(s) AFFECTED (Positive or negative)	EFFECT *(for stakeholder)*	AFFECTED STAKEHOLDERS (Positive or negative)
- Automated attacks - Targeted attacks	- Anonymity (-) - Subscriber privacy (-) - Freedom (-) - Cash (-) - System damage (+) - Personal data(+)	- Attacker looses anonymity if the attack is detected. *If attack is successful:* - Attacker gains one or more of the assets he wants. - Risks freedom	- Difi Mangement(-) - Difi ICT (-) - Users (-) - Regulatory Services (-) - Competitors (+)
- Buy personal data - Hack accounts - Register new user with unregistered birthnumbers (in Difi DB)	- Anonymity (-) - Cash (-) - Subscriber privacy (-) - Personal data (+) - Sensitive personal data (+) - Birth numbers (+)	- Attacker runs risk of loosing anonymity, when he interacts directly with traders, or interacts directly with the system. - Attacker gains personal data and birth numbers and use this for further attacks or data mining.	- Difi Mangement(-) - Difi ICT (-) - Users (-) - Regulatory Services (-) - Competitors (+) - Internal threat actors (+)

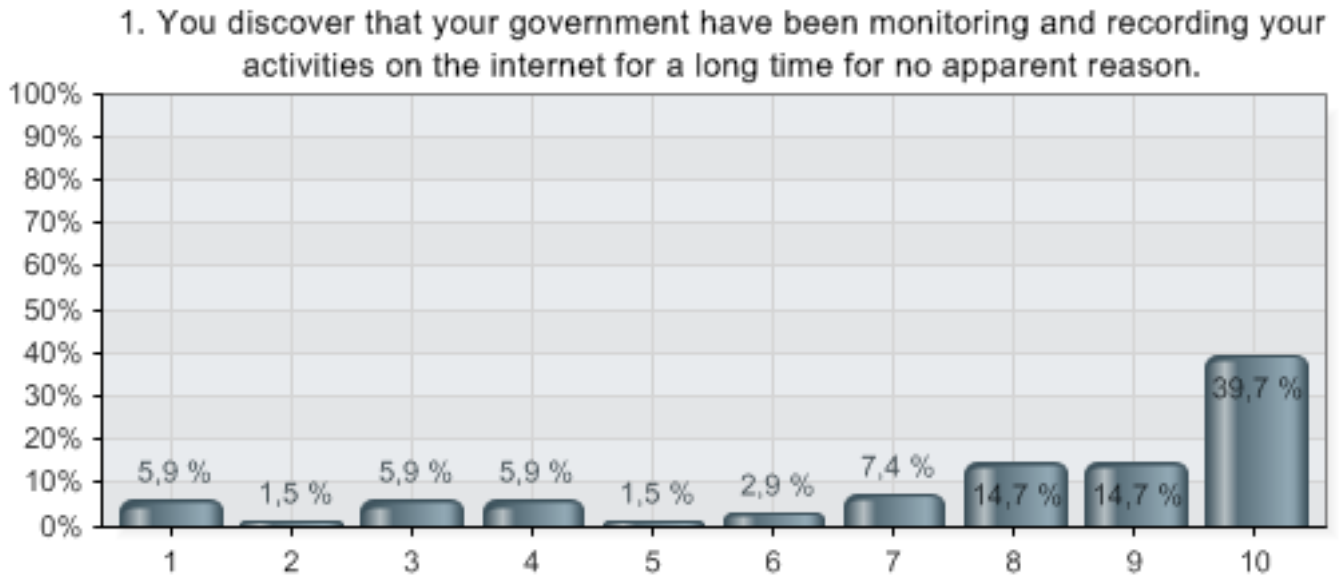
E Appendix - Questionnaire

Documentation of 20 questions and answers from the questionnaire named "Rating of Privacy Risks".

Rating of Privacy Risks

Published from 25.04.2012 to 25.04.2012
68 responses (1 unique)

1. You discover that your government have been monitoring and recording your activities on the internet for a long time for no apparent reason.

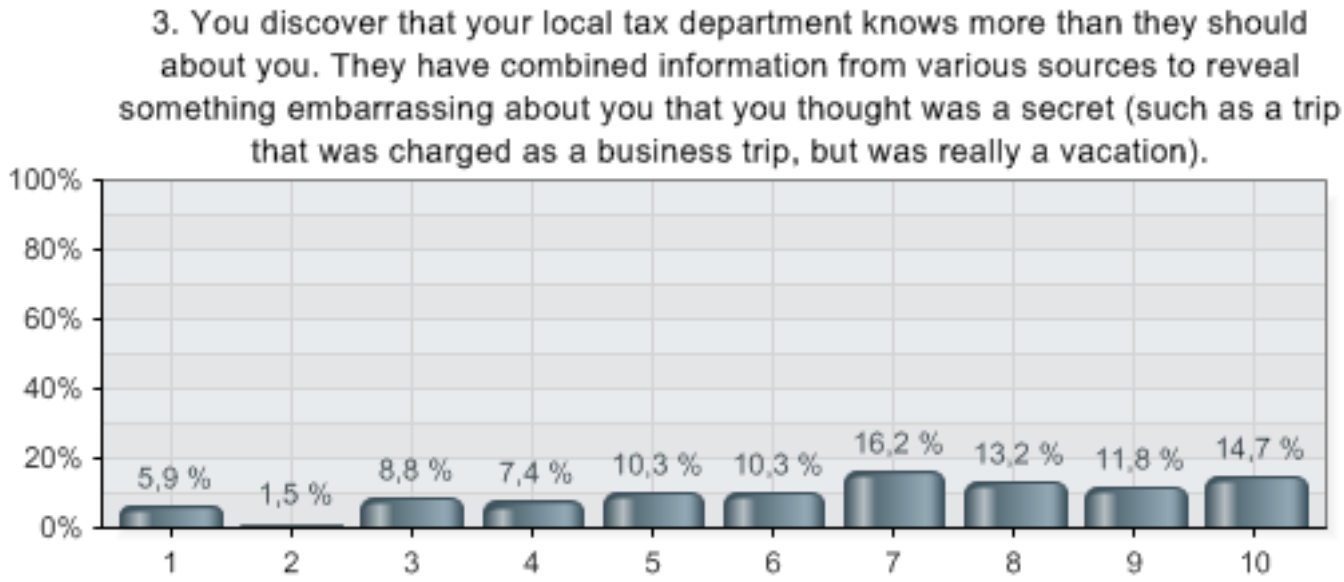


Alternatives	Percent	Value
1 1	5,9 %	4
2 2	1,5 %	1
3 3	5,9 %	4
4 4	5,9 %	4
5 5	1,5 %	1
6 6	2,9 %	2
7 7	7,4 %	5
8 8	14,7 %	10
9 9	14,7 %	10
10 10	39,7 %	27
Total		68

2. During a job interview; you feel pressured to reveal a piece of personal information about yourself in order to get the job that you would rather have kept secret.

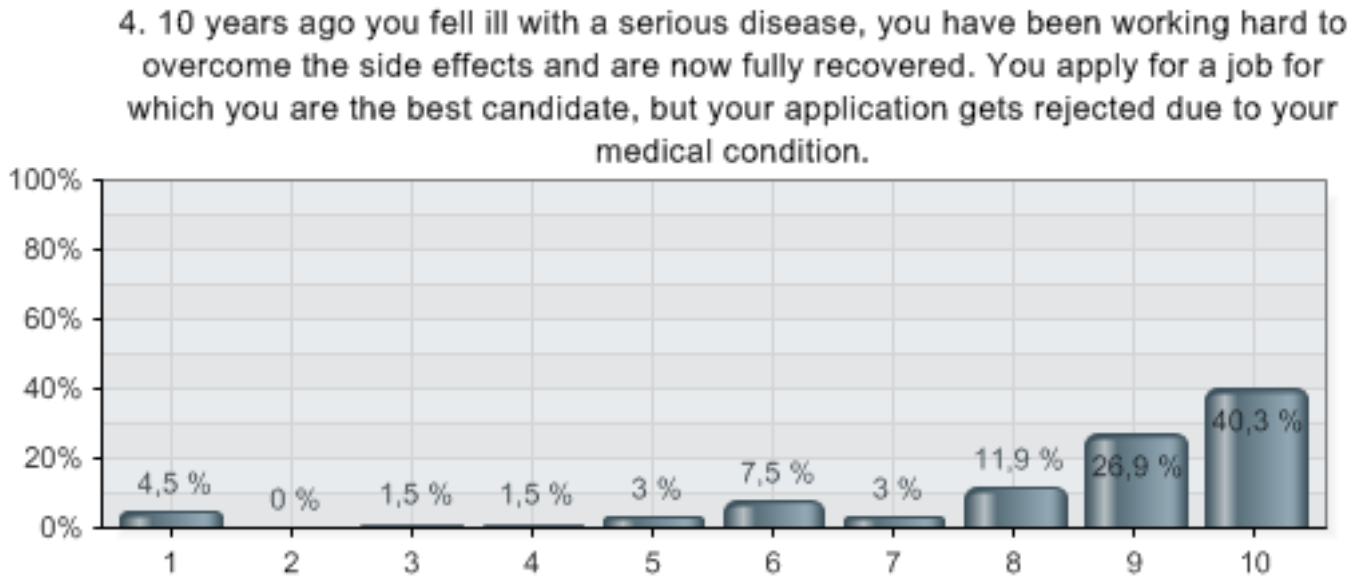
Alternatives	Percent	Value
1 1	2,9 %	2
2 2	4,4 %	3
3 3	5,9 %	4
4 4	7,4 %	5
5 5	10,3 %	7
6 6	11,8 %	8
7 7	14,7 %	10
8 8	19,1 %	13
9 9	13,2 %	9
10 10	10,3 %	7
Total		68

3. You discover that your local tax department knows more than they should about you. They have combined information from various sources to reveal something embarrassing about you that you thought was a secret (such as a trip that was charged as a business trip, but was really a vacation).



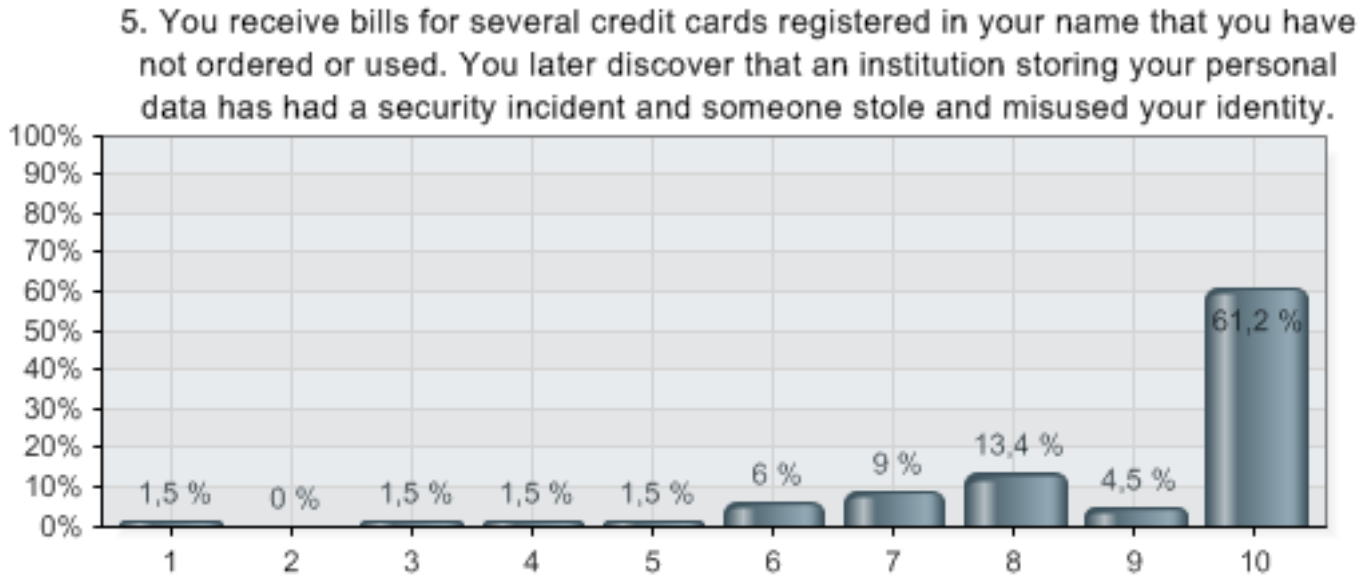
Alternatives	Percent	Value
1 1	5,9 %	4
2 2	1,5 %	1
3 3	8,8 %	6
4 4	7,4 %	5
5 5	10,3 %	7
6 6	10,3 %	7
7 7	16,2 %	11
8 8	13,2 %	9
9 9	11,8 %	8
10 10	14,7 %	10
Total		68

4. 10 years ago you fell ill with a serious disease, you have been working hard to overcome the side effects and are now fully recovered. You apply for a job for which you are the best candidate, but your application gets rejected due to your medical condition.



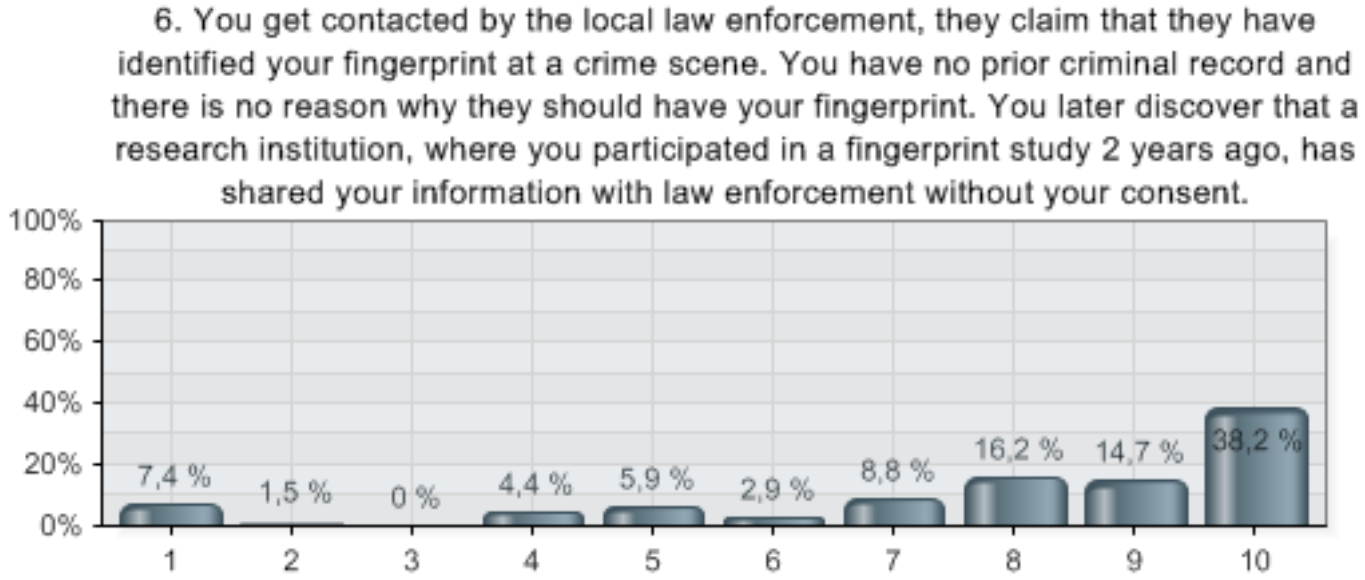
Alternatives	Percent	Value
1 1	4,5 %	3
2 2	0,0 %	0
3 3	1,5 %	1
4 4	1,5 %	1
5 5	3,0 %	2
6 6	7,5 %	5
7 7	3,0 %	2
8 8	11,9 %	8
9 9	26,9 %	18
10 10	40,3 %	27
Total		67

5. You receive bills for several credit cards registered in your name that you have not ordered or used. You later discover that an institution storing your personal data has had a security incident and someone stole and misused your identity.



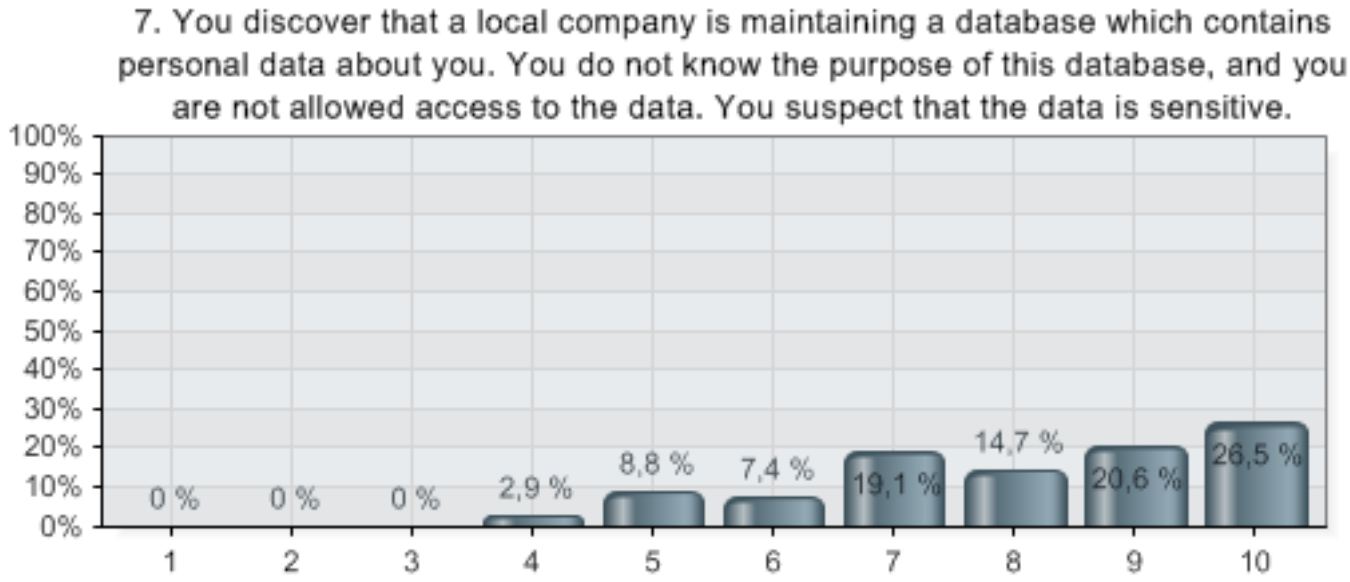
Alternatives	Percent	Value
1 1	1,5 %	1
2 2	0,0 %	0
3 3	1,5 %	1
4 4	1,5 %	1
5 5	1,5 %	1
6 6	6,0 %	4
7 7	9,0 %	6
8 8	13,4 %	9
9 9	4,5 %	3
10 10	61,2 %	41
Total		67

6. You get contacted by the local law enforcement, they claim that they have identified your fingerprint at a crime scene. You have no prior criminal record and there is no reason why they should have your fingerprint. You later discover that a research institution, where you participated in a fingerprint study 2 years ago, has shared your information with law enforcement without your consent.



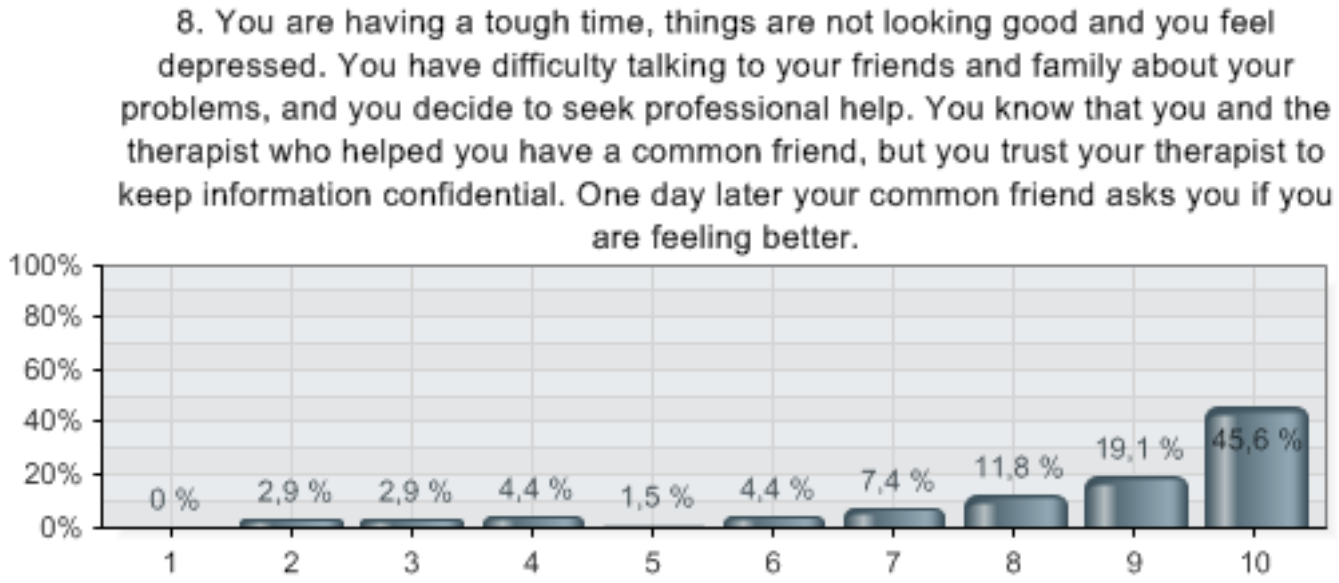
Alternatives	Percent	Value
1 1	7,4 %	5
2 2	1,5 %	1
3 3	0,0 %	0
4 4	4,4 %	3
5 5	5,9 %	4
6 6	2,9 %	2
7 7	8,8 %	6
8 8	16,2 %	11
9 9	14,7 %	10
10 10	38,2 %	26
Total		68

7. You discover that a local company is maintaining a database which contains personal data about you. You do not know the purpose of this database, and you are not allowed access to the data. You suspect that the data is sensitive.



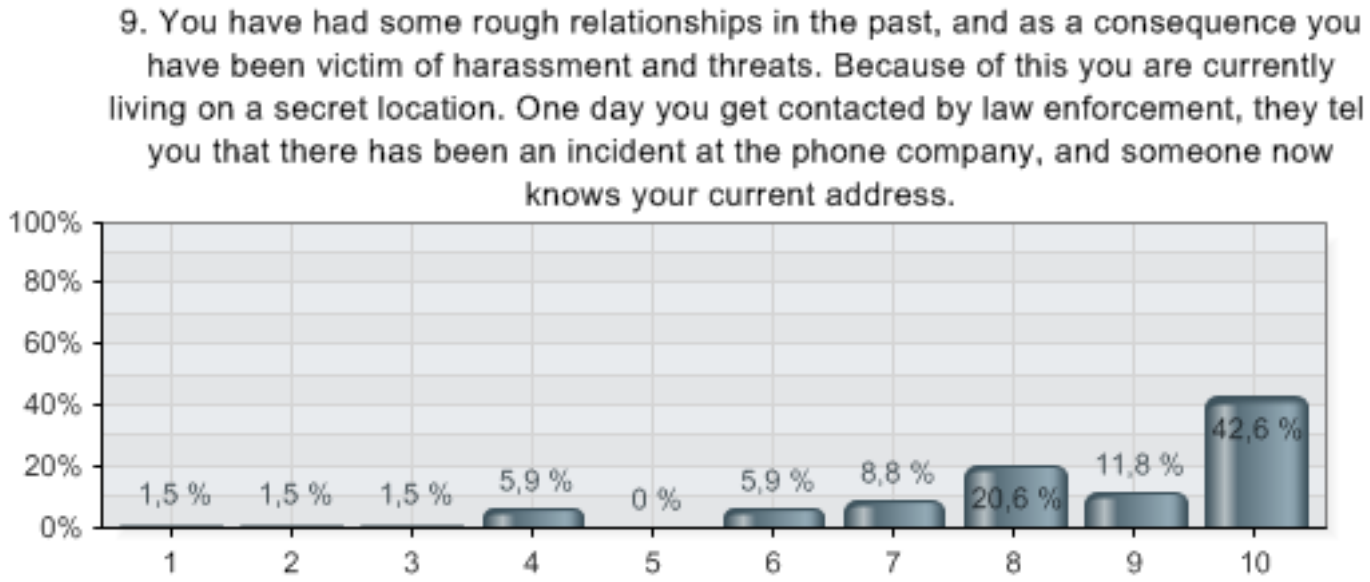
Alternatives	Percent	Value
1 1	0,0 %	0
2 2	0,0 %	0
3 3	0,0 %	0
4 4	2,9 %	2
5 5	8,8 %	6
6 6	7,4 %	5
7 7	19,1 %	13
8 8	14,7 %	10
9 9	20,6 %	14
10 10	26,5 %	18
Total		68

8. You are having a tough time, things are not looking good and you feel depressed. You have difficulty talking to your friends and family about your problems, and you decide to seek professional help. You know that you and the therapist who helped you have a common friend, but you trust your therapist to keep information confidential. One day later your common friend asks you if you are feeling better.



Alternatives	Percent	Value
1 1	0,0 %	0
2 2	2,9 %	2
3 3	2,9 %	2
4 4	4,4 %	3
5 5	1,5 %	1
6 6	4,4 %	3
7 7	7,4 %	5
8 8	11,8 %	8
9 9	19,1 %	13
10 10	45,6 %	31
Total		68

9. You have had some rough relationships in the past, and as a consequence you have been victim of harassment and threats. Because of this you are currently living on a secret location. One day you get contacted by law enforcement, they tell you that there has been an incident at the phone company, and someone now knows your current address.

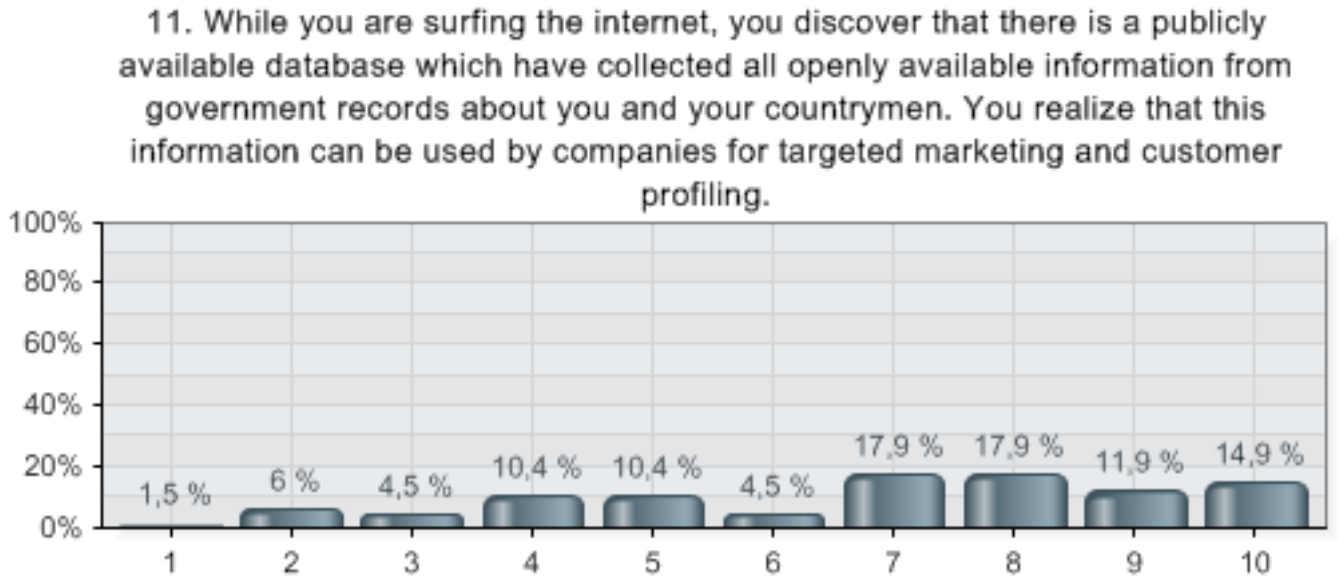


Alternatives	Percent	Value
1 1	1,5 %	1
2 2	1,5 %	1
3 3	1,5 %	1
4 4	5,9 %	4
5 5	0,0 %	0
6 6	5,9 %	4
7 7	8,8 %	6
8 8	20,6 %	14
9 9	11,8 %	8
10 10	42,6 %	29
Total		68

10. Last night you had a bit too much to drink, you do not remember much of what happened. But when you turn on your computer, you find that your friends have posted a revealing picture of you on a public website, where you are relieving yourself of bodily fluids.

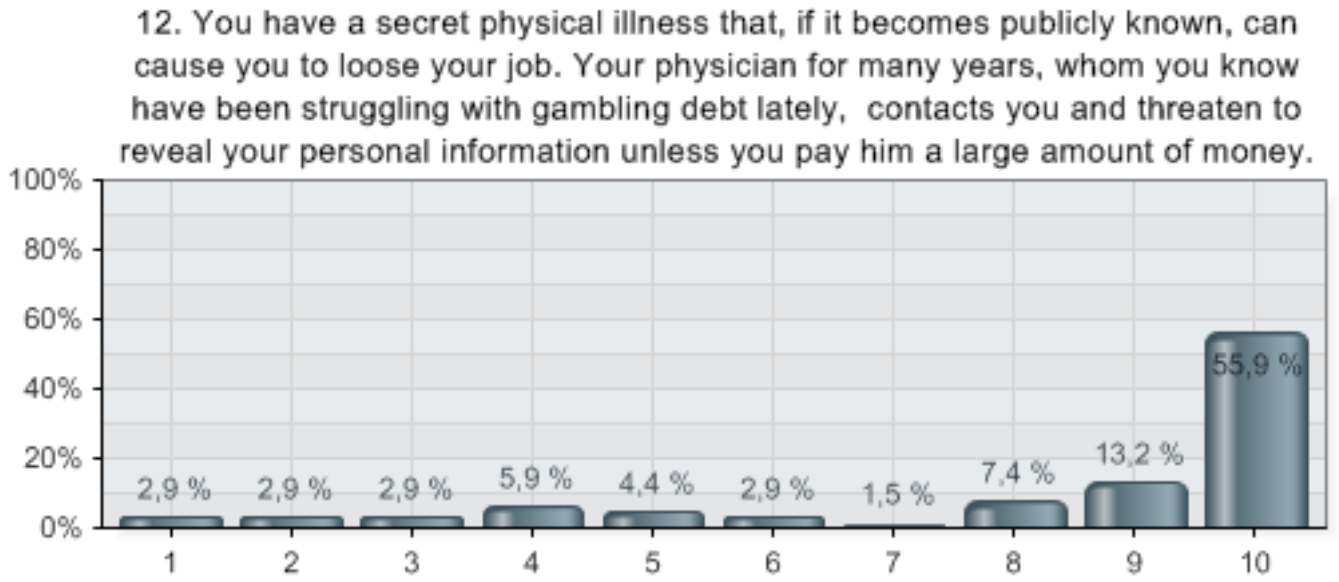
Alternatives	Percent	Value
1 1	2,9 %	2
2 2	0,0 %	0
3 3	2,9 %	2
4 4	2,9 %	2
5 5	4,4 %	3
6 6	11,8 %	8
7 7	13,2 %	9
8 8	17,6 %	12
9 9	8,8 %	6
10 10	35,3 %	24
Total		68

11. While you are surfing the internet, you discover that there is a publicly available database which have collected all openly available information from government records about you and your countrymen. You realize that this information can be used by companies for targeted marketing and customer profiling.



Alternatives	Percent	Value
1 1	1,5 %	1
2 2	6,0 %	4
3 3	4,5 %	3
4 4	10,4 %	7
5 5	10,4 %	7
6 6	4,5 %	3
7 7	17,9 %	12
8 8	17,9 %	12
9 9	11,9 %	8
10 10	14,9 %	10
Total		67

12. You have a secret physical illness that, if it becomes publicly known, can cause you to loose your job. Your physician for many years, whom you know have been struggling with gambling debt lately, contacts you and threaten to reveal your personal information unless you pay him a large amount of money.

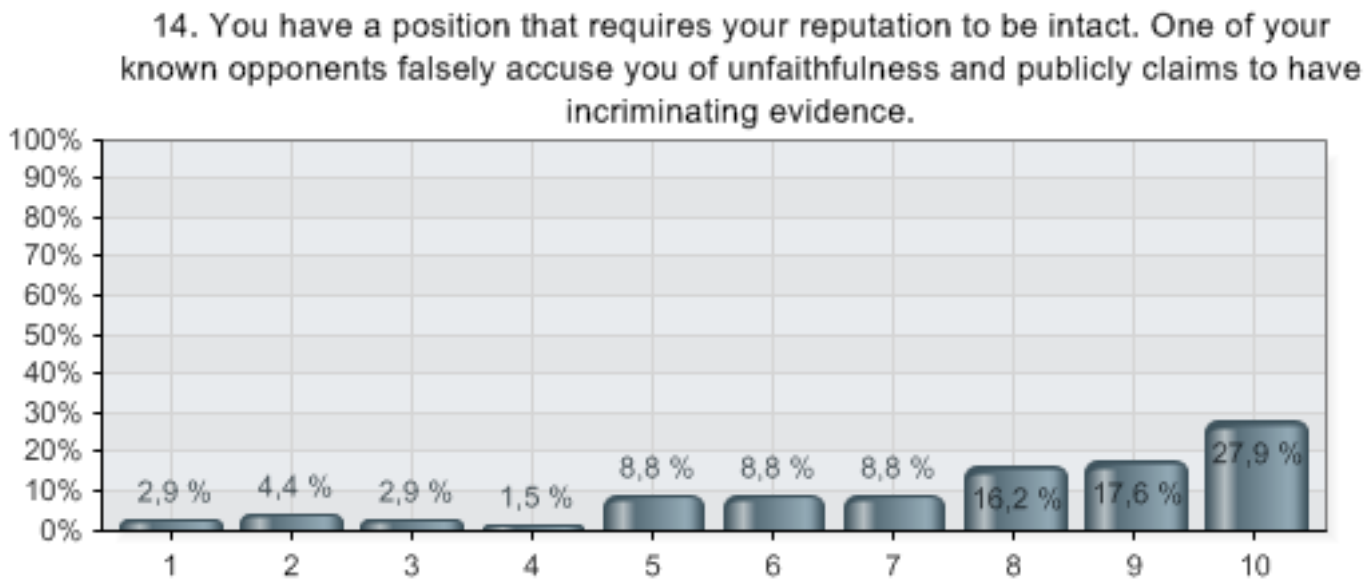


Alternatives	Percent	Value
1 1	2,9 %	2
2 2	2,9 %	2
3 3	2,9 %	2
4 4	5,9 %	4
5 5	4,4 %	3
6 6	2,9 %	2
7 7	1,5 %	1
8 8	7,4 %	5
9 9	13,2 %	9
10 10	55,9 %	38
Total		68

13. You are "forced" by your significant other to join in on a charity event which you do not support. A picture of you is taken during this event. Some weeks later you discover your picture in a magazine, where it is being used in a commercial for the charity organization. Your beliefs and opinions differ greatly from the organization, and you do not wish to be associated with them.

Alternatives	Percent	Value
1 1	4,5 %	3
2 2	3,0 %	2
3 3	4,5 %	3
4 4	6,0 %	4
5 5	7,5 %	5
6 6	9,0 %	6
7 7	10,4 %	7
8 8	23,9 %	16
9 9	10,4 %	7
10 10	20,9 %	14
Total		67

14. You have a position that requires your reputation to be intact. One of your known opponents falsely accuse you of unfaithfulness and publicly claims to have incriminating evidence.

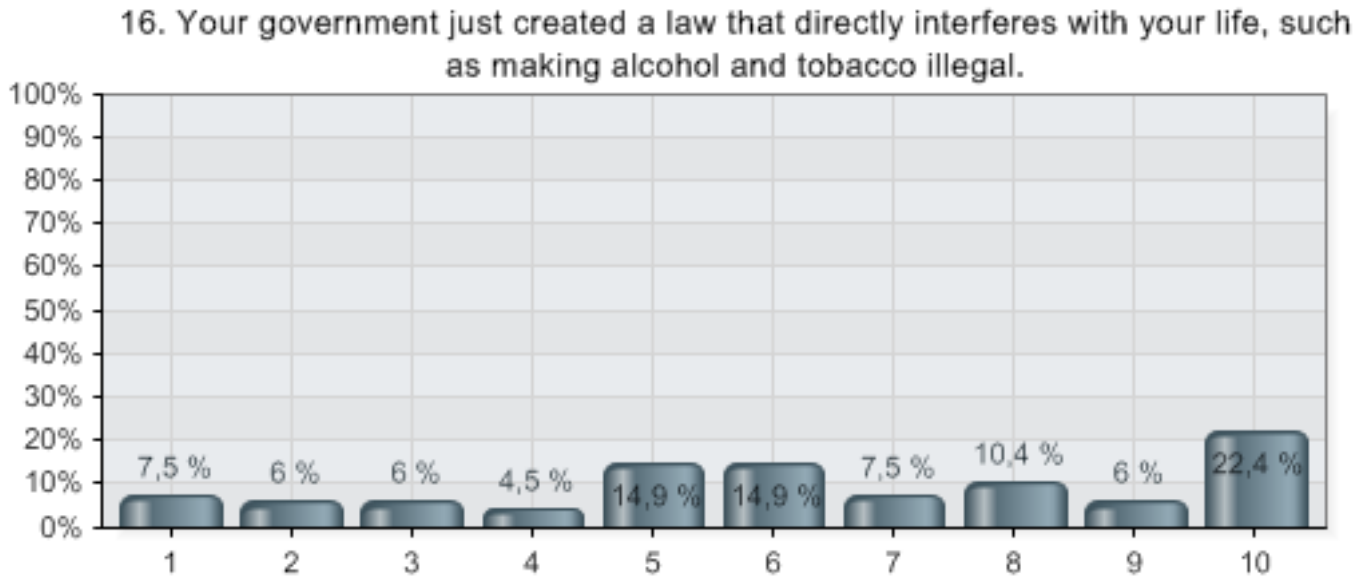


Alternatives	Percent	Value
1 1	2,9 %	2
2 2	4,4 %	3
3 3	2,9 %	2
4 4	1,5 %	1
5 5	8,8 %	6
6 6	8,8 %	6
7 7	8,8 %	6
8 8	16,2 %	11
9 9	17,6 %	12
10 10	27,9 %	19
Total		68

15. You have accomplished one of your life goals, and as a result you have become famous. A bi-product of new-found fame is that you are constantly being photographed by paparazzi, and as a result you and your family is constantly in the media spotlight.

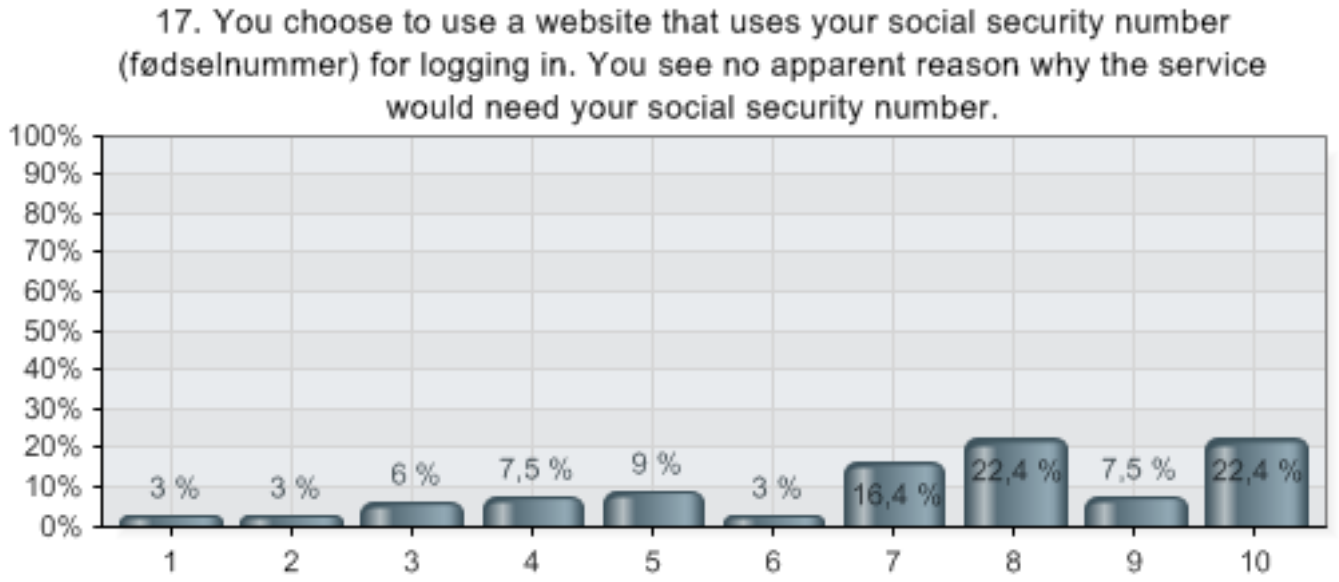
Alternatives	Percent	Value
1 1	2,9 %	2
2 2	7,4 %	5
3 3	10,3 %	7
4 4	5,9 %	4
5 5	7,4 %	5
6 6	11,8 %	8
7 7	16,2 %	11
8 8	16,2 %	11
9 9	7,4 %	5
10 10	14,7 %	10
Total		68

16. Your government just created a law that directly interferes with your life, such as making alcohol and tobacco illegal.



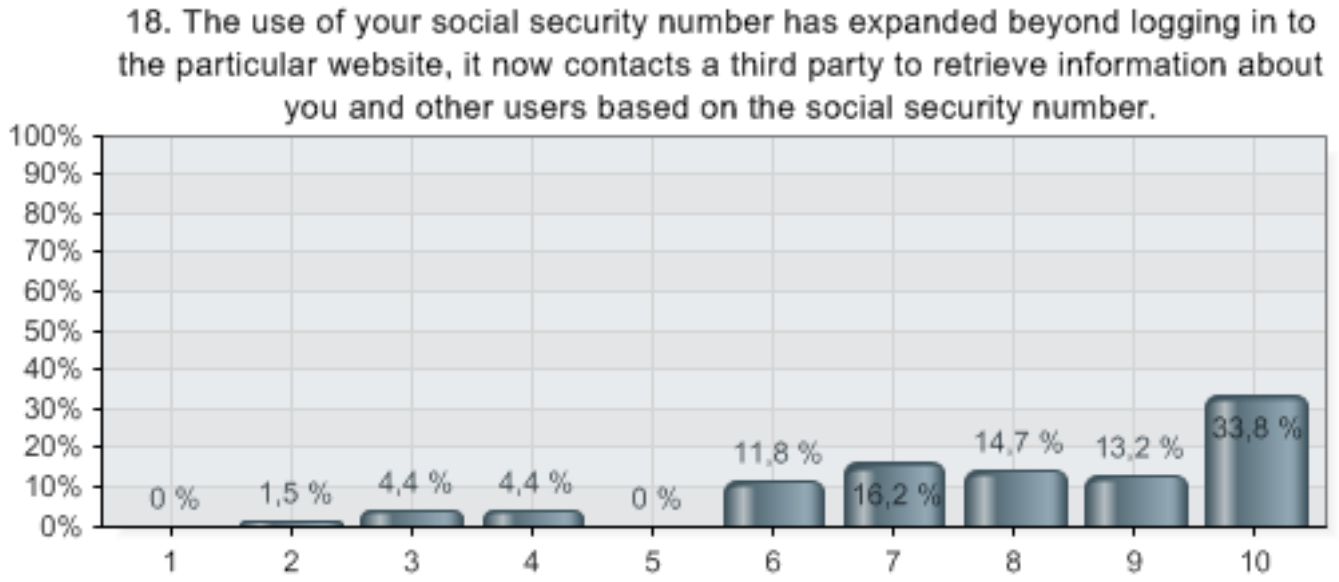
Alternatives	Percent	Value
1 1	7,5 %	5
2 2	6,0 %	4
3 3	6,0 %	4
4 4	4,5 %	3
5 5	14,9 %	10
6 6	14,9 %	10
7 7	7,5 %	5
8 8	10,4 %	7
9 9	6,0 %	4
10 10	22,4 %	15
Total		67

17. You choose to use a website that uses your social security number (fødselnummer) for logging in. You see no apparent reason why the service would need your social security number.



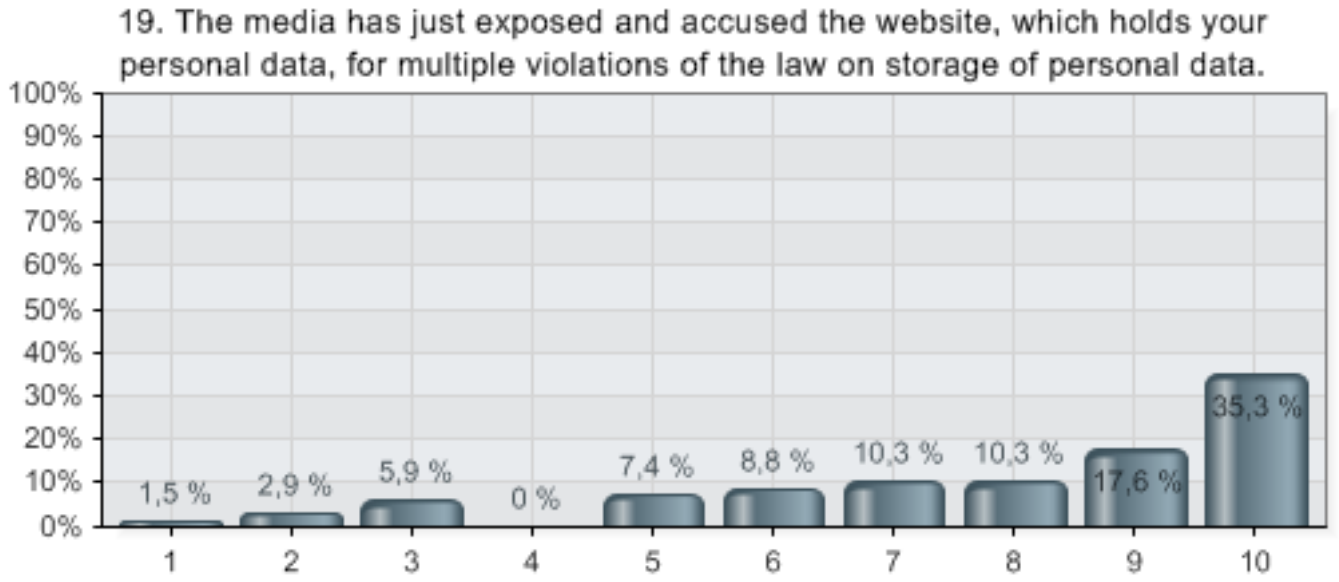
Alternatives	Percent	Value
1 1	3,0 %	2
2 2	3,0 %	2
3 3	6,0 %	4
4 4	7,5 %	5
5 5	9,0 %	6
6 6	3,0 %	2
7 7	16,4 %	11
8 8	22,4 %	15
9 9	7,5 %	5
10 10	22,4 %	15
Total		67

18. The use of your social security number has expanded beyond logging in to the particular website, it now contacts a third party to retrieve information about you and other users based on the social security number.



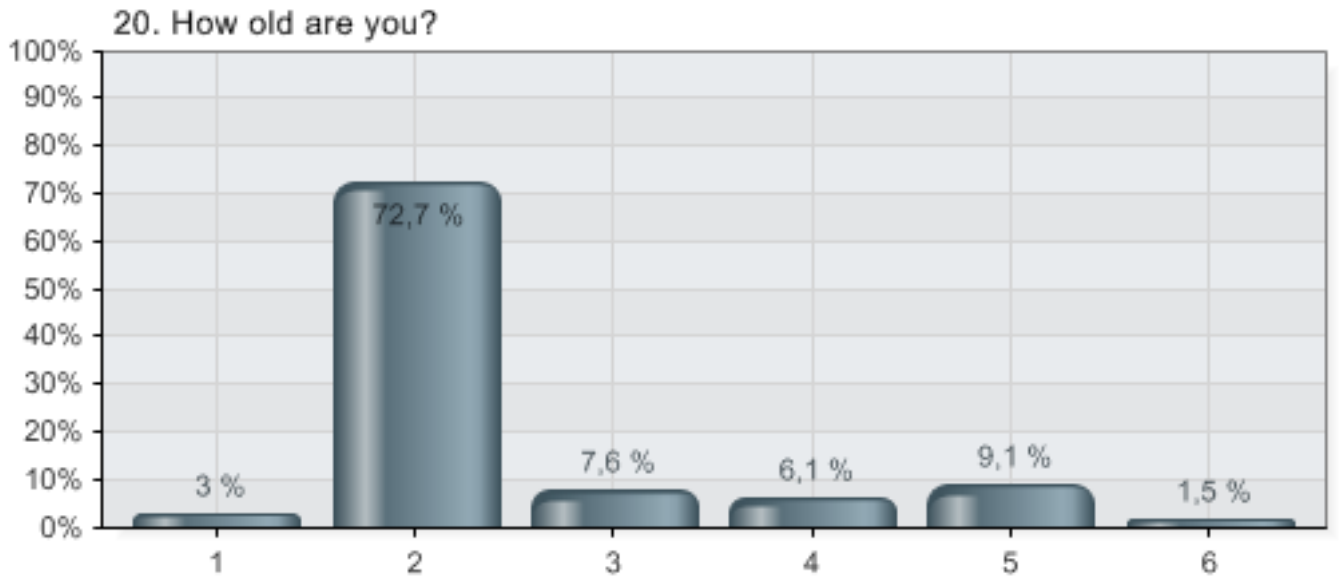
Alternatives	Percent	Value
1 1	0,0 %	0
2 2	1,5 %	1
3 3	4,4 %	3
4 4	4,4 %	3
5 5	0,0 %	0
6 6	11,8 %	8
7 7	16,2 %	11
8 8	14,7 %	10
9 9	13,2 %	9
10 10	33,8 %	23
Total		68

19. The media has just exposed and accused the website, which holds your personal data, for multiple violations of the law on storage of personal data.



Alternatives	Percent	Value
1 1	1,5 %	1
2 2	2,9 %	2
3 3	5,9 %	4
4 4	0,0 %	0
5 5	7,4 %	5
6 6	8,8 %	6
7 7	10,3 %	7
8 8	10,3 %	7
9 9	17,6 %	12
10 10	35,3 %	24
Total		68

20. How old are you?



Alternatives	Percent	Value
1 19 or younger	3,0 %	2
2 20-29	72,7 %	48
3 30-39	7,6 %	5
4 40-49	6,1 %	4
5 50-59	9,1 %	6
6 60 and above	1,5 %	1
Total		66

F Appendix - Difi Correspondance

Correspondance with Difi customer service to help determine personal infomation present in their high level logs.

APPENDIX 1

Copy of e-mail correspondance with Difi concerning content of logs (in norwegian)

From: <brukerstotte@difi.no>
To: "Gaute Wangen" <gautebw@hotmail.com>
Subject: (Ref. nr:2373880) Spørsmål om lagring av personopplysninger
Date: 19. mars 2012 15:49

(Ver vennlig å behold tittel når du svarer på denne e-post)

Hei.

IP-adressen blir ikke logget sammen med informasjon om vellykkede innlogginger og endringer, men det er andre logger hvor IP-adresse og tidspunkt lagres. Disse loggene er det færre i Difi som har tilgang til, og kan brukes til å etterforske hendelser ved behov.

Du kan også kontakte MinID brukerstøtte på grønt nummer 800 30 300.

Vi har åpent alle hverdager kl. 8–17.

Vanlige_spørsmål_og_brukermanualer.

Vennlig hilsen

Postboks 8115 Dep., 0032 Oslo
Telefon: 800 30 300/ www.difi.no

Gaute Wangen 2012-03-16 15:27:07:
>
> Hei,
>
>
> takk for svar.
>
> Med tanke på sporbarhet, logger dere IP-adressen sammen med tidspunkt for
> hver innlogging?
>
>
>
> mvh
> Gaute Wangen
>
>
>
>
>
> From: brukerstotte@difi.no
>
>
> Sent: Thursday, March 15, 2012 10:58 AM
>
>
> To: Gaute_Wangen
>
>
> Subject: (Ref. nr:2373880) Spørsmål om lagring av personopplysninger

>
>
>
>
>
> Hei.
>
>
> Informasjon som logges om brukere av MinID er tidspunkt for registrering
og
> samtykke, endring av opplysninger som f.eks mobil og e-post, og tidspunkt
> og annen relevant informasjon for vellykket innlogging til en tjeneste.
>
>
> Loggene brukes kun til statistikk, og for sporbarhet slik at man kan
> oppdage hva som har skjedd f.eks ved feil eller andre hendelser.
>
>
> Du kan også kontakte MinID brukerstøtte på grønt nummer 800 30 300.
>
>
> Vi har åpent alle hverdager kl. 8–17.
>
>
> Vanlige__spørsmål_og_brukermanualer.
>
>
> Vennlig hilsen
>
>
> Postboks 8115 Dep., 0032 Oslo
> Telefon: 800 30 300/ www.difi.no
>
>
> Gaute Wangen 2012-03-12 13:48:53:
>>
>> Hei,
>
>> jeg ser på siden
>> http://www.difi.no/elektronisk-id/minid/sikkerhet-og-personvern, at
dere
>> logger informasjon om min bruk av MinID (sitat: “For å beskytte deg mot
>> misbruk og feil logger vi også informasjon om din bruk av MinID”).
>>
>> Jeg lurer på hvilken informasjon dere lagrer i disse loggene?
>>
>> Mvh
>>
>>
>> Gaute Wangen
>
>

G Appendix - Hour list

This appendix contains the documentation of work hours for conducting the Privacy Impact Assessment and Risk IT assessment.

Date	Hours	Theme
		PIA
28.02.2012	8	Initial assessment
29.02.2012	8	Initial assessment
01.03.2012	0	Initial assessment
02.03.2012	7,5	Initial assessment
05.03.2012	7,5	Initial assessment
06.03.2012	6	Initial assessment
07.03.2012	7,5	Initial assessment
08.03.2012	7,5	Initial assessment
09.03.2012	7,5	Initial assessment
12.03.2012	4	Initial assessment
13.03.2012	7,5	Initial assessment
	71	
15.03.2012	3	Preliminary phase
16.03.2012	7	Preliminary phase
16.04.2012	4	Preliminary phase
	14	
31.03.2012	4	Preparation phase Stakeholder analysis
01.04.2012	7,5	Preparation phase Stakeholder analysis
02.04.2012	8	Preparation phase Stakeholder analysis
03.04.2012	6,5	Preparation phase Stakeholder analysis
10.04.2012	9	Preparation phase Stakeholder analysis
11.04.2012	8	Preparation phase Stakeholder analysis
12.04.2012	8	Preparation phase Stakeholder analysis
	51	
17.04.2012	2	Analysis and consultation phase
18.04.2012	8	Analysis and consultation phase – Mehari Risk Analysis
19.04.2012	9	Analysis and consultation phase – Mehari Risk Analysis
20.04.2012	4	Analysis and consultation phase – Mehari Risk Analysis
21.04.2012	7	Analysis and consultation phase – Mehari Risk Analysis
	30	
24.04.2012	8	Documentation phase
25.04.2012	4	Documentation phase
26.04.2012	9	Documentation phase
	21	
		Risk IT
30.04.2012	9	Risk IT – Risk Universe
01.05.2012	5	Risk IT – Risk Identification
02.05.2012	8	Risk IT – Risk Identification
03.05.2012	10	Risk IT – Risk Identification (4) + Analysis (6)
04.05.2012	6	Risk IT – Risk Analysis
07.05.2012	4	Risk IT – Complete report
	42	