Privacy challenges in AMS/Smart Grid

Aud Gran

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2013

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

Privacy challenges in AMS/Smart Grid

Aud Gran

2013/11/27

Abstract

The traditional power grid has served well in its existing period by transmitting and distributing electricity from centralized generators to consumers. Characteristics of this grid has been a one-way flow of energy and energy meters that have to be read manually. Environmental and societal challenges rises new demands for a more effective and flexible solution for energy distribution. Motivated by the combat against global warming and desire for national energy independence a smart power grid is in development. Smart Grid (SG) is regarded as the new generation power grid by utilizing modern information technologies to enable a two-way communication between advanced smart meters and head-end systems at utility companies. While conventional power grids are generally used to carry power form central generators to the users, SG uses two-way flow of power and information to deliver electricity in a more flexible, reliable and cost-effective way.

For SG fulfil its purposes, information communicated through Advanced Meter Infrastructure (AMI) is much more fine-grained than the every two months readings in the traditional grid and can because of that reveal information about habits and activities inside the resident based data of electricity usage. This is a severe challenge in regard of the privacy of energy consumers, and is a problem utility companies must address in the deployment of SG and Advanced Metering Systems (AMS).

Collection of data classified as sensitive and personal is regulated by laws, but there are grey zones between clearly illegal and legal data collection, storage and use. The purpose of data collection must be clearly defined and communicated to the data subjects. The challenges in regard of privacy in SG development are several, from creating a secure communication channel for transporting data between the smart meters and the head-end systems and to establish a trust amongst the energy consumers so they can feel safe that their personal information is not compromised or misused.

This thesis takes a closer look at the concept of privacy in the context of AMS and SG and explores the threats and vulnerabilities of privacy that exists in this infrastructure. Based on this the thesis presents results from interviews with several Distribution System Operators (DSO) where they have been asked how they address privacy challenges in their AMS projects and how they regard privacy concerns in the future power grid.

Sammendrag

Det tradisjonelle strømnettet har fram til i dag hatt oppgaven med å overføre og distribuere elektrisitet fra sentrale kraftstasjoner og ut til forbrukerne. Dette nettet kjennetegnes ved enveis flyt av energi og strømmålere som må avleses manuelt. Miljøhensyn og samfunnsutfordringer i forhold til kapasitet og beredskap har etterhvert framkalt et behov for en mer fleksibel, robust og effektiv løsning for distribusjon av elektrisitet. Motivert av kampen mot global oppvarming og et ønske for nasjoner å være energiuavhengige, er et smartere strømnett under utvikling. Smart grid (SG) anses som den nye generasjonen av strømnett der det tas i bruk moderne informasjonsteknologi for to-veis kommunikasjon mellom avanserte smarte målere og systemene hos nettselskapene. Mens det tradisjonelle nettet brukes for å frakte strøm ut til kundene, benytter SG informasjonsteknologi for å sende både informasjon og energi begge veier, og oppnår en mer fleksibel, robust og økonomisk løsning.

For å oppnå formålet med SG og AMS (avanserte måle-system) er målerverdiene som sendes mellom måler og nettselskap målt med høyere frekvens enn den tradisjonelle avlesningen annen hver måned, og kan derfor utlede mye informasjon om hvilke vaner og aktiviteter beboerne i husstanden har, basert på forbruk av elektrisitet. Dette er en stor utfordring med tanke på personvernet til forbrukerne og er et element som nettselskapene må håndtere i planleggingen og utviklingen av det nye strømnettet.

Innsamling av data som er klassifisert som sensitiv og personlig informasjon er stengt regulert av lovverket, men det er gråsoner mellom det som er tillatt og det som er klart ulovlig innsamling, lagring og bruk av disse dataene. Formålet være tydelig definert og kommunisert til forbrukerne. Utfordringene når det gjelder personvern i SG er mange, fra å etablere sikre kommunikasjonskanaler mellom måler og nettselskapenes systemer, til å etablere tillit hos forbrukerne på at den personlige informasjon ikke misbrukes eller spres.

Denne masteroppgaven ser nærmere på personvern i AMS og smart grid og presenteres trusler og sårbarheter for personvernet i infrastrukturen. Med dette som grunnlag vil rapporten presentere resultatene fra en intervjuundersøkelse med flere nettselskaper hvor de ble spurt om hvordan de håndterer personvernutfordringene i AMS prosjektene, og hvordan de ser på personvern i den videre utviklingen av AMS.

Acknowledgements

I would like to thank my supervisor Lasse Øverlier for his support, feedback and guidance during my period of writing this thesis. I would also like to thank all the lecturers and other employees at Gjøvik University College who makes it possible for remote part-time students to complete a Masters Degree. My gratitude also goes to my employer, Mære Landbruksskole, for giving me the opportunity and flexibility to combine work and study.

I would also like to thank the respondents participating in my interview project; Anne Sagstuen Nysæther, Project Manager AMS at Eidsiva Energi Nett AS, Morten Bjerkan, Project Manager AMS at NTE Nett AS, Vidar Kristoffersen, AMS Project Owner at Fredrikstad Energi Nett AS, Halvard Glad, Project Manager AMS at Tromskraft Nett AS and Tarjei Benum Solvang, Project Manager AMS at Nordlandsnett AS. Without your openness and positive attitudes to attend to the interviews this thesis would not have been written. I will also express my gratitude to Gunnar Bådsvik and his family for giving me access to his smart meter data.

My fellow students Roger Larsen and Ernst Kristian Henningsen have been indispensable sources of encouragement, collaboration and laughter during this years since we started on the Master of Science in Information Security. You have been fantastic partners in crime.

Finally I want to give my biggest thank to my family and friends who has supported me throughout these years. I give a special thank-you-kiss to my Ketil who has been an important discussion partner, supported me and listened to my frustration without any complaints.

Last but absolutely not least, I want to dedicate this thesis to my wonderful children, Konrad(9) and Wilma(2), who have been sharing their mum with this thesis for a long time. You have thought me the art efficiency and kept my feet on the ground when the world seemed to circle around me, myself and my thesis.

Abbreviations

AMS	- Advanced Metering Systems
AMI	- Advanced Metering Infrastructure
DSO	- Distribution System Operator
EDC	- Electricity Distribution Company
HES	- Head End System
NSGC	- Norwegian Smart Grid Centre
NUSP	- Non-Utility Service Providers
NVE	- Norwegian Water Resources and Energy Directorate
PbD	- Privacy by Design
PLC	- Power Line Carrier
SCADA	- Supervisory Control And Data Acquisition
SG	- Smart Grid

Contents

List of Figures

List of Tables

1 Introduction

This chapter serves as an introduction to this master thesis. First it gives a short presentation of the thesis topic and problem description, then a brief description of justifications and finally the results and knowledge the project aims to achieve.

1.1 Topic

The Norwegian Distribution System Operators(DSO) are in the process of planning and implementing the new Advanced Metering System (AMS) and enabling two-way flow of information and electricity between energy production and consumers. This is as a part of a new smart grid. Modern information technology is used to deploy a cyber-layer on top of the existing power grid and the goal is to achieve a more efficient, flexible, robust and cost-effective grid.

Communication of information from nodes and sensors in AMS are important to make this new system feasible, and a key component is the smart meter that replaces the traditional electricity meter in every metering point in the power grid. Smart meters measures electricity usage and communicates this information back to the DSO. The data is fine-grained and has the potential to reveal information about household activities, which raises severe challenges in regard of privacy.

Legislation, as the personal Data Act among others, regulates when and how personal information can be collected and used for different purposes. In figure 1, clearly illegal situations are illustrated by the red area where information is collected and used illegally. The green area illustrates legal situations. But there are grey areas between legal and illegal handling of personal information that should be discussed and clarified before systems are deployed, and AMS is one of those systems. In AMS there are conflicting interest between privacy preservation and availability of data from smart meters to use in management and operation of the power grid [5]. Privacy is a complex and hard to define because it is connected to personal experiences and culture. It is therefore important to raise knowledge and awareness of how privacy can be compromised and of the consequences threats and vulnerabilities might lead to.

The topic of this thesis is the privacy challenges evolving from the deployment of AMS and how they are addressed by the industry. Zhuo Lu et al. (2010) [7] categorize malicious threats towards the SG network into three types based on their goals: (1) network availability, (2) data integrity and (3) information privacy. This projects topics will fall into the last category.

1.2 Keywords

Privacy, smart grid, AMS, AMI, smart meter, information security.

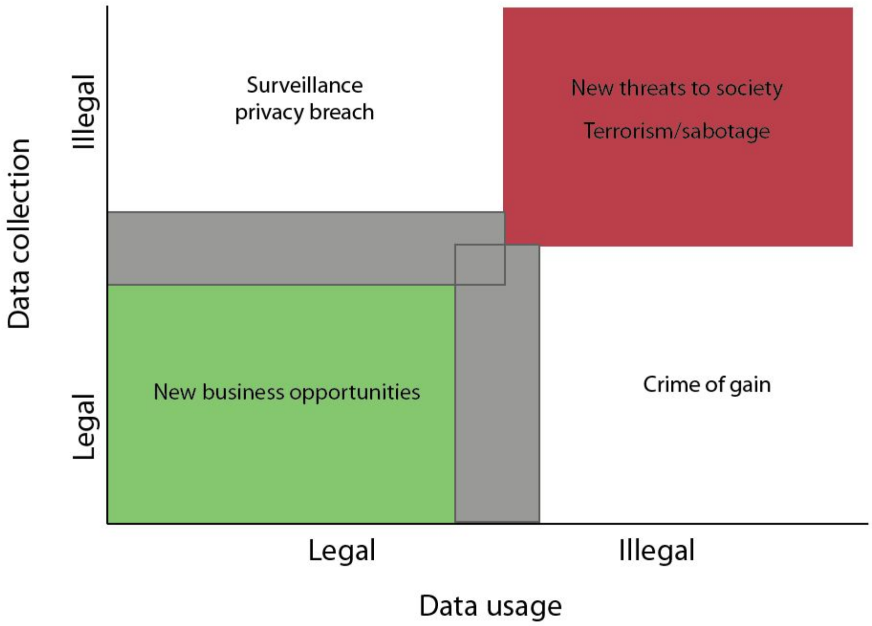

Figure 1: Grey areas of collection and use of data from smart meters. (source: arena smart grid services)

1.3 Problem description

To make the features of AMS and SG possible, large amounts of data about the consumers energy usage are collected at requested time intervals by smart meters in their homes. Smart meters or third-party devices can also have interfaces to electrical appliances, like water heater or air conditioner, which can enable a convenient remote control, but also puts them on line and open for monitoring.

This detailed data can disclose information about activities and habits in the household, and for instance by the use of load signature algorithms it is possible to extract information about what appliances are at use at any given time [8, 9]. Collecting, storing and processing personal data in Norway are regulated by the Personal Data Act [10] but business seeks to create value from personal information, and the quality of data is essential. This leads to a competitive privacy problem, where there is a conflict between the utility companies using data to maximize their management potential and the privacy of the consumers [11,12]. The challenge is to ensure that the line between legal an illegal collection and use of such data is not crossed and consequently lead to violation of privacy.

1.4 Justification, motivation and benefits

The objectives of AMS is to modernize the power grid to meat existing and upcoming energy and climate challenges and to make the energy distribution more robust and flexible. These purposes are strong forces behind AMS deployment and it is important to hinder that privacy is ignored when SG adds new functionality to conventional electricity grids. Utility companies and third-party vendors have interests in smart meter data for operational or commercial reasons, hence it is important to consider privacy as a part of the overall security planning when AMS is deployed.

There are grey zones between legal and illegal collection and use of personal information. Technological security can to a certain degree be purchased for money, but privacy is also a social and cultural concept where there are no off the shelf solution for ensure security. It is important to debate this in advance and during AMS development because social boundaries of what is right and wrong when it comes to privacy varies and shifts when new technology is adopted.

The data collected by smart meters reflects the power usage in the home of the consumer. This can tell e.g. whether the user are at home and what his habits are. This rises questions about privacy challenges, and this project will examine threats on privacy related to collection, transmission and use of data in the advanced Metering Infrastructure (AMI). AlAbdulkarim and Lukszo (2011) [13] defines consumers privacy as an example of social vulnerabilities that might influence the system and its goals. The energy consumers are the obvious stakeholders in this project, but it is also of interest of utility companies and power suppliers to take privacy challenges serious in AMS, because consumer's trust and acceptance is of vital importance.

As a mean to combat energy challenges, SG will develop fast during the next years and new privacy challenges will arise. As a networked society we must consider these possible challenges and make sure that legal, moral and social measures are taken to ensure the security of personal information. How the final deployment of AMS systems handles private information will be a result of legislative means, guides, norms in the industry and knowledge.

1.5 Research questions

1. What are the privacy challenges in AMS and smart grid?
2. How is privacy addressed by the Distribution System Operators (DSO)?
3. What data is captured, transferred and stored by smart meters and AMI related to electricity usage, and can these data be used or misused to deduce information in a format that it threatens the privacy of the consumers?
4. The development of smart grid will increase during the next years, and new applications might find commercial use of the opportunities that evolve from this. How can the society be prepared to handle future privacy challenges arising from smart grid?

1.6 Contributions

The main focus of this thesis is to examine how the privacy challenges originating from development of AMS and SG are handled in the AMS projects in Norway. AMS deployment are, at the time of writing this thesis, by most of the Norwegian DSOs ongoing projects, and the deadline for complete implementation is January 1st 2019. Therefore the progress of the deployment will reflect the results.

By answering the research questions this thesis aims to help understand the complexness of privacy and how this is an issue in AMS. The results from interviews with DSOs will be discussed to give knowledge of how DSOs address privacy in AMS so far in the deployment, and present suggestions to what the authorities, the industry and energy consumers can do in order to preserve privacy in the new power grid.

1.7 Thesis outline

The thesis will first give a theoretical foundation and discussion of related work to give a better understanding of the research questions. Further it will present results from qualitative interviews, followed by a discussion of the results and a conclusion.

- Chapter 2 explains the terms smart grid and AMS to give a theoretical foundation to the qualitative interviews.
- Chapter 3 aims to explain the complex nature of privacy and what problems privacy violations can cause.
- Chapter 4 gives a brief presentation of laws and regulation with relevance to privacy in AMS.
- Chapter 5 summaries threats and vulnerabilities in AMS according to smart meter data.
- Chapter 6 explains the methodology used to answer the research questions.
- Chapter 7 presents the results from interviews with five AMS project managers in different DSOs.
- Chapter 8 discussed the results from the interview project.
- Chapter 9 and 10 is the conclusion of this thesis and presents proposed future work.

2 Smart grid and AMS

This chapter gives a short presentation of the concepts of smart grid and AMS as a foundation to the discussion of privacy vulnerabilities in chapters 5, and as supplementary information to the interview project in chapter 7.

2.1 What is smart grid and AMS?

The traditional power grid are used to carry power from central generators to a large number of customers by supporting operations like electricity generation, transmission, distribution and control. The new generation electricity grid is called smart grid (SG) and uses two-way flows of electricity and information to create an advanced energy delivery network that supports the vision of a sustainable and reliable future energy system [2, 5]. Digital systems are used to enhance customers and utility companies ability to monitor, control and predict energy use. The modern technology makes it possible for the SG to distribute power in more efficient ways and enables more control for responding to conditions and incidents. Table 1 gives a comparison of features of the traditional power grid and SG. A definition of SG stated in the article by Gharavi and Ghafurian (2011) [14] describes SG as an electric system that uses information, two-way, cyber-secure communication technologies, and computational intelligence in an integrated fashion across electricity generation, transmission, substations, distribution and consumption to achieve a system that is clean, safe, secure, reliable, resilient, efficient and sustainable.

SG does not replace the existing power grid, but builds on the existing infrastructure to increase utilization of existing assets and to empower the implementation of new technology.

Existing grid	**Smart Grid**
Electromechanical	Digital
One-way communication	Two-way communication
Centralized generation	Distributed generation
Few sensors	Sensors throughout
Manual monitoring	Self-monitoring
Manual restoration	Self-healing
Failures and blackouts	Adaptive and islanding
Limited control	Pervasive control
Few customer choices	Many customer choices

Table 1: Comparison between the existing power grid and smart grid [5]

Advanced Metering System (AMS) is the system where smart meters are installed on the metering points in customers homes. The meters communicates data about energy usage and operational data between end-users equipment and head end systems (HES) at the DSO. AMS is not the same as SG, but a key component among others that constitutes SG.

2.1.1 Motivation

The global population is growing and there is an increased demand for electricity and a stable supply of energy. Existing power grids are under pressure and the motivations behind the deployment of SG is connected to both environmental and operational aspects.

Effective power grid management

In the traditional power grid, the DSO does not have detailed information available from the distribution network. SG provides much more information about the situation of energy demands and the state of the infrastructure which enables the utility companies to operate the grid with more efficiency and optimized system operations. By analysing information from SG together with for instance temperature data, DSOs are able to perform better planning and make optimal investments. Because power distribution is a service critical to society, the properties of smart grid is advantageous in regard of contingency and retaining a stable energy supply.

Environmental concerns

It is a global concern for the environment to reduce carbon dioxide (CO_2) emission and counteract the effect of global warming. Governments wants to increase the utilization of renewable energy sources and increase energy efficiency. SG enables more distributed production with two-way flow of electricity. In existing electricity infrastructure there is centralized approach where central stations distribute energy out to the consumers. In order to tackle the rising need for energy and complying with economic and social demands, the society moves against more use of renewable energy from smaller and decentralized resources [15]. Distributed generation of energy is not automatically clean, but it is an important property of smart grid that it is prepared to handle such energy production.

Customer control of energy usage

At the local level there is a purpose to let home users actively manage their energy usage by enabling time-of-use prizing. The result is that the customers energy costs varies in regard of the energy prizes at the time of use. In that way the customers can reduce their electricity costs by using high energy demanding equipment when the prizes are low [16]. By letting the customers be able to control their energy costs, the goal is to reduce the periods with the highest peaks of energy usage.

2.1.2 Deployment of AMS

The Norwegian regulator, The Norwegian Water Resources and Energy Directorate (NVE), has determined rules for providing complete large-scale deployment of smart meters and AMS by January 1st, 2019. During 2013 the deadline was postponed from 2017 to 2019 due to the need for the DSOs to do more planning, gain positive effects from technological development and to clarify unanswered questions. For the rest of Europe, the goal is to implement smart meters in all households with 80% completion by 2020 and 100% by 2022.

Demo projects

Prior to the final implementation of AMS in Norway, national projects of demo areas has been established in collaboration between DSOs and the Norwegian Smart Grid Centre (NSGC). The two sites mentioned in this thesis is Demo Steinkjer [17] and Smart Energy Hvaler [18]. They are both national projects where actors can perform testing and research on solutions and technology under realistic conditions for use in future AMS implementations. Demo Steinkjer is owned by NTE Holding AS and is operated by NTE Nett AS. Smart Energi Hvaler is a collaboration between Fredrikstad Energi AS, Hvaler local government and NCE Smart Energy Markets. By establishing these demo sites, the industry can prepare for several challenges in AMS deployment by gaining useful experience and results from research projects.

Centralized hub for AMS data in Norway

Statnett is the system operator in the Norwegian energy system and is a state enterprise. In an assessment of common IT solutions for exchanging AMS data in connection with the AMS deployment, Statnett recommended a common centralized hub for storage of smart meter data accessible for all DSOs and electricity suppliers. Main functionality of the hub is storage and distribution of electricity usage data, and a place where customers can change their electricity suppliers and control invoice balancing [19]. A hub for the Norwegian market is decided to be put into operation within October 2015, and Statnett has signed a letter of intent with Danish Energinet.dk to evaluate the possibilities of deployment of a common solution [20].

2.2 Architecture

Smart grid is as mentioned earlier in this chapter, a modern electricity grid where information technology is used to gather and act on information in an automated way. The architecture of smart grid is shown in figure 2, where information and communication technology connects the energy chain from energy production to transmission and distribution to end users. It also enables connection of micro grids of localized systems of power generation which also can function autonomously. Information collected from the system enables a high level of control of the functionality of the grid [1].

Figure 3 shows an example of a AMS infrastructure [2] and illustrates how different communication technologies are used to send data from home smart meters to the DSOs ICT systems. Data can be collected directly from the smart meters, or via concentrators or master meters where data is collected from several metering points before transmitted to HES.

Figure 4 illustrates the infrastructure of the AMS with a more detailed description of the components. The meter is connected to the system at a metering point and registers electricity as a part of the meter node. The metering terminal includes a communication module for transmission of data and stores data until transmission is completed. The switch for choking functionality is used to reduce or choke outlet of electricity in the metering node [21]. According to regulation, the meter must be equipped with a standardized port for external connection of for instance a separate display, control unit or other types of meters.

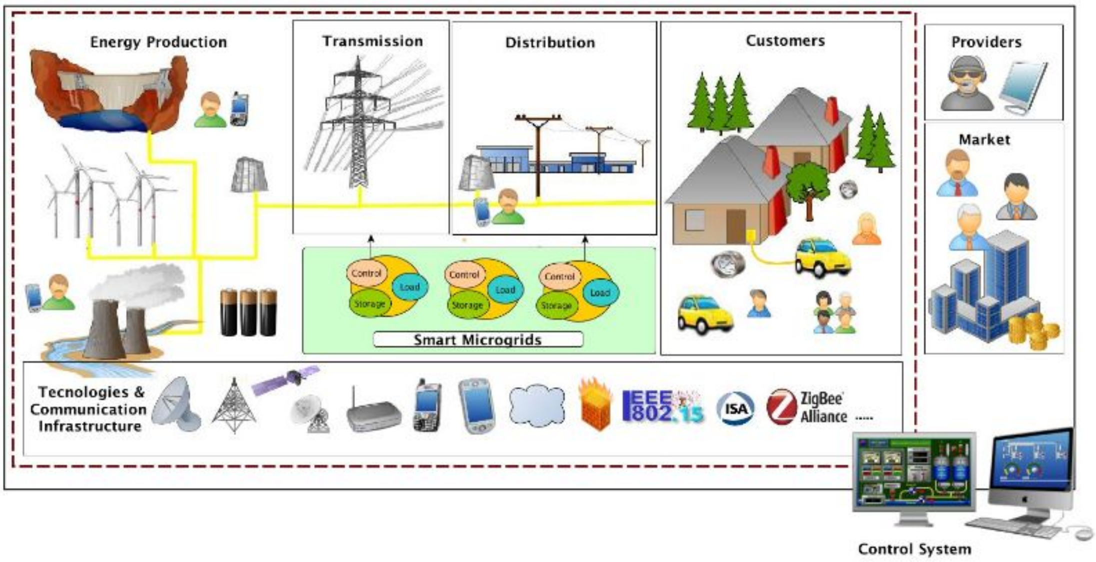

Figure 2: Smart grid architecture [1]

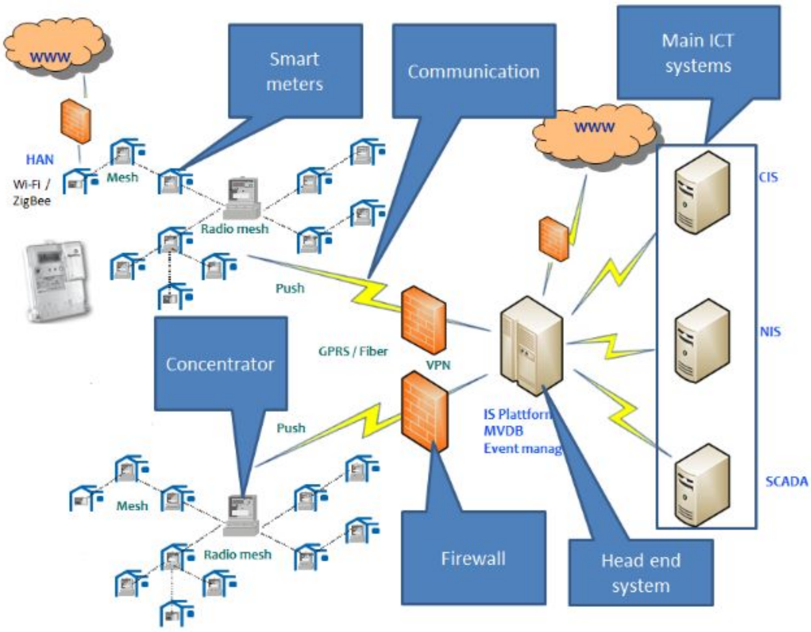

Figure 3: Example of AMS infrastrukture. Smart energy Hvaler [2]

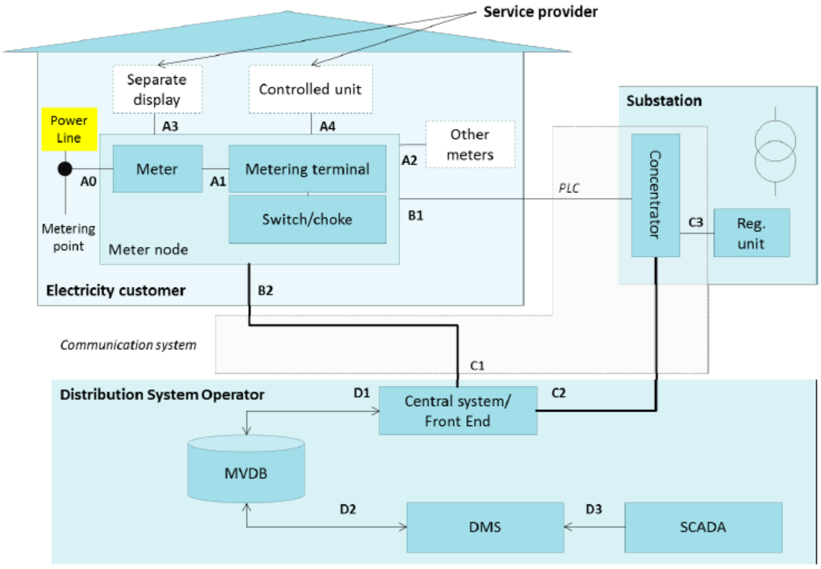

Figure 4: Advanced metering infrastructure [3]

2.3 Distribution System Operators and Non-Utility Service Providers

Distribution System Operators (DSOs) in Norway operates in a monopolistic market under regulations from the directorate (NVE). The companies have licences for a given area to build and operate the power distribution grid. The license obliges the DSO to provide electric energy to all the customers in that area [22]. Besides the grid operation and obliged tasks, DSOs do not provide other commercial services to the customers in regard of their energy usage.

Data from smart meters contains much information and are valuable for DSOs in their grid management, but also third party companies, also known as Non-Utility Service Providers (NUSP) will have an interest in providing new products and services directly to the customer based on their data of energy usage. NUSPs interacts directly with the energy consumers and offer non-utility products and services where the consumer provides the data directly to the NUSP [23].

Interfaces for such products includes for instance metering devices and web portals. Examples of products and services are electric efficiency analysis and energy management systems, like *iControl* from iControl Networks and *SmartMonitoring* from AlertMe. One important feature of these products and services is to make use of fine grained meter data and enable customers to have continuously access to information about their energy usage. Vulnerabilities according to smart meter data will be discussed in more detail in chapter 5.

2.4 Internet of things

The Internet is changing and evolving and new applications and businesses are continuously being created. Technology changes the internet with cheaper and wider spread broadband, smaller, less costly and more powerful devices are equipped with a variety of on board sensors and communication interfaces. This situation where more and more devices becomes connected is the new paradigm called the Internet of Things (IoT). IoT is a result of the expansion of internet through inclusion of physical objects combined with the ability to provide smarter services to the environment as more data becomes available [24].

Using IoT technology in SG is an important approach to enable the flow of information in power grid systems which is motivated by the need to have an effective management of the power grid infrastructure. Power Internet of Things (PIoT) is the application of IoT in SG and can achieve reliable information transmission through wired or wireless network and smart information processing in all parts of the power chain, from generation to consumption [25]. In order to realize the visions of SG, an important element is to have continuous monitoring and control. Functionality offered by the networked embedded devices that realises this constant flow of information is crucial to the success of SG, for instance the smart meters for monitoring energy consumption. As a result from the exchange of information, today we have devices communicating their functionality status [15]. A vision in SG is that devices can behave based on shared information, for instance a water heater turning on the power only when energy prices are below a predefined threshold.

Threat implications

There are challenges on several levels in a system where everything is connected, especially in regard of privacy. When all things are networked and communicates information about their local environment to a central location this becomes a situation with similarities of surveillance, since information about humans can be collected in a direct or indirect fashion. This connectivity carries with it a risk to privacy and information leakage [24]. Information in IoT is widely distributed throughout the system, so that any successful capture of one system will likely result in capture of information to which that system has access. Wide distribution of communication might result in a longer chain or a dense mesh of communication, giving attackers opportunities to intercept in the transmission of information. Applications in IoT and SG will provide unobtrusive access to information about users and their environment. A good deployment of these systems will depend on our ability to secure them and the contextual data they share [26]. Due to the topology of SG and IoT and the fact that more and more devices and appliances are connected to the internet raises new vulnerabilities that did not exist in the traditional power grid. An overview and a short discussion of these vulnerabilities will be the subject of chapter 5.

2.5 Smart grid data

Data from smart meters installed in energy consumers homes collects information about usage and quality (voltage) of electricity in the metering point. According to the Energy Regulation [27], meters must be able to measure usage with a granularity of 60 minutes, with options to change the measuring frequency to 15 minutes. This accumulates a very big amount of data, which can deduce information compromising the privacy of habitants of the house [28].

2.5.1 Data analysis example

As an example of how AMS meter data of energy usage can deduce information about the activities in a house, meter data from Demo Steinkjer was obtained from NTE Nett AS in order to perform a simple analysis. In the first analysis performed anonymized data was used. On such data it is possible to make profiles over time and to see habits and routines for when people are at home using electricity or not, but the result from the analysis can not be confirmed.

To perform an analysis where the profile and findings can be confirmed, data from an identified customer was needed. Identifiable data was obtained from the DSO by making an agreement with a customer living in the demo area. Data was handed out in exchange for a signed declaration from the customer.

The data was in a listed format of hourly measured metering values of electricity usage over a period from September 2012 to September 2013. By using Microsoft Excel and its pivot table function, the data could be analysed to see trends an profiles of activities in regard of energy consumption in the house. Following are some examples of information that was deduced from this data.

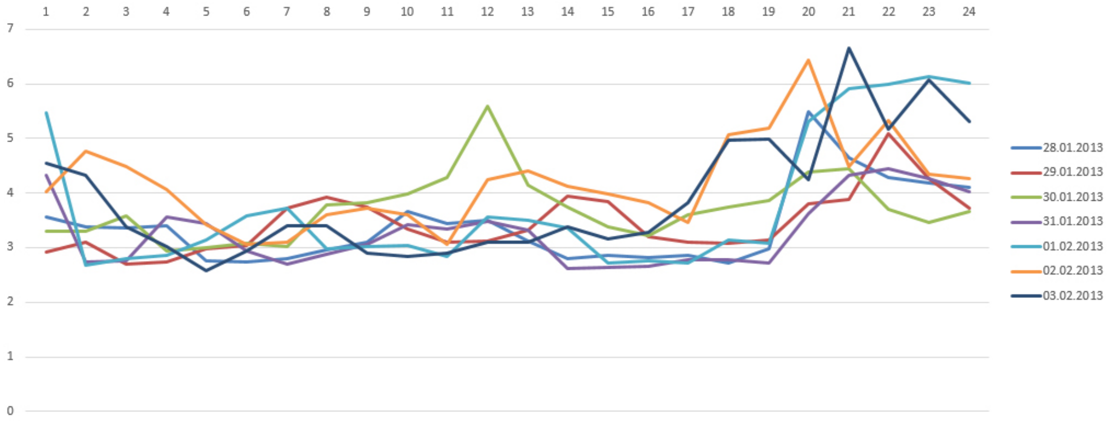

Figure 5: Example of hourly measured data for one week.

Figure 5 shows an example of a normal week of work hours and activities (Energy usage in kWh per hour, and hours 1-24 starting at 1 AM.). The illustration shows that the electricity usage falls after midnight when the household is sleeping. At 6 AM they wake up, does their morning rituals, showering and making breakfast, and leaves for work. At about 5 AM they return back home to make dinner and doing other electricity consuming activities. Hence a profile for a work day can be deduced by measuring the average usage over several days, illustrated in figure 6.

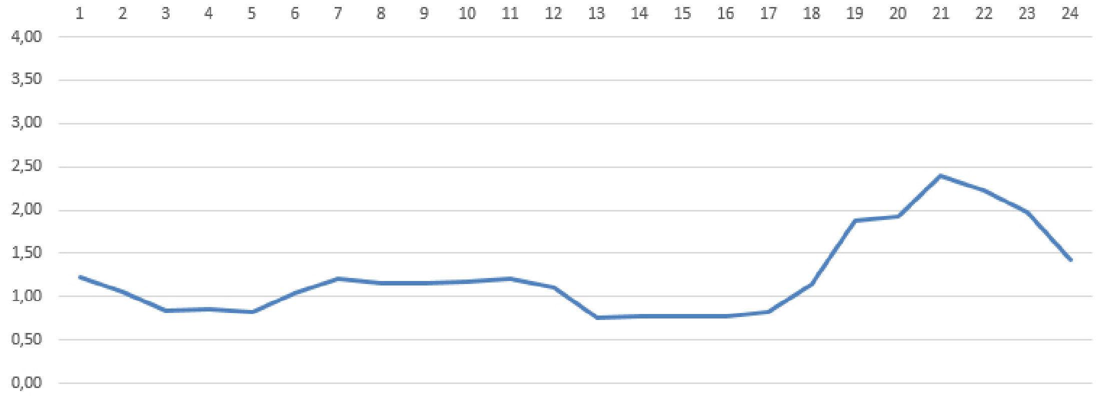

Figure 6: Profile of average energy usage on workdays.

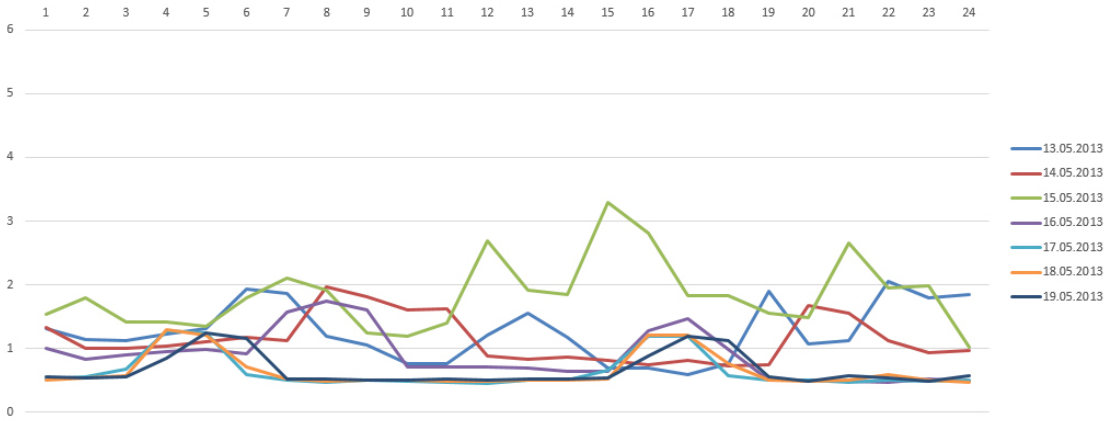

Figure 7: Week 20, Norwegian National Day 17th of May

During the data analysis, it showed that there was peak in energy usage on every Wednesday in the period from 9-11 AM and for some hours, also seen as the green curve in figure 5 and 7. The profile for only Wednesdays showed a different curve than other workdays, with a obvious increase of energy usage during morning and mid day. This indicates that somebody is at home on these days. The owner of the house could explain this as his wife, working from about 8 AM to 17-19 AM on weekdays, has a day off every Wednesday and often did activities like washing clothes.

The periods of nobody being home for some time longer than a day was very easy to find. An example is shown in figure 7 where the family was away from the house during the weekend of the Norwegian National Day on 17th of May.

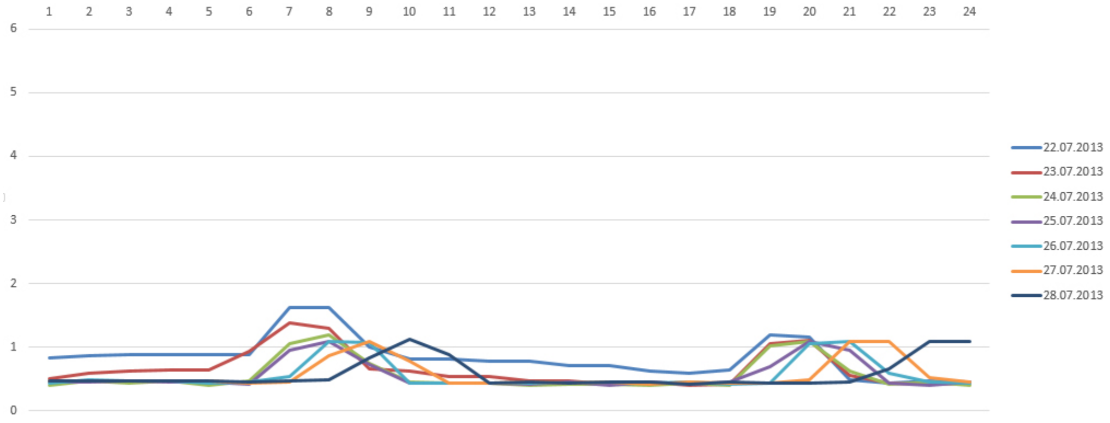

Figure 8: Week of vacation.

Situations where the family is on vacation and away from the house for a longer period of time have a characteristic profile, seen in figure 8. The curve of energy usage has only a couple of bumps during the day which is a result of the water heater turning on and off.

There were also possible to spot several times where the energy usage reached very high peaks. A challenge in the process of finding the reasons for such abnormal energy usage was off course for the habitants of the house to remember what had happened back in time.

The data used in this experiment was hourly measured. According to the Energy Act Regulation [27], all AMS meters installed in Norway must have the capability to be configured to measure energy usage in 15 minutes frequency. In a situation of data with 15 minutes granularity there will be even easier to deduce detailed information about the household activities.

3 Privacy

This chapter discusses the concept of privacy, how it has changed through history and how new technology has lead to a whole new spectre of vulnerabilities. The chapter also presents a taxonomy of activities that impinge upon privacy [4]. This framework will be used later in this thesis to classify privacy challenges in smart grid. This chapter is based on a literature study to get a good knowledge of privacy in order to answer the first and fourth research question from section 1.5.

According to the Norwegian Data Protection Authority, privacy can be explained as *the right to a private life and the right to control your own personal information* [29]. The right to privacy is established in The Universal Declaration of Human Rights article 12: *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks* [30]. Legislation regulates how and when personal information can be collected, stored and used, and the owners rights to control this data. Despite fundamental rights and clear legislation there are privacy challenges all over the society. One reason for this is the fact that privacy is a concept that is complex and vague at the same time and therefore difficult to define. It is something that affects us in our everyday activities but if we are asked to describe what privacy is, it is hard to cover every aspect of it. Daniel J. Solove [4] claims that privacy is a concept in disarray, and does not fare well when pitted against more concretely stated countervailing interests. In order to say why privacy is important and should be protected there is a need to have a clearer understanding of what privacy violations means. Only then we can address the challenges in protecting our privacy the right way.

3.1 Historic and contemporary perspectives on privacy

Trust and privacy are ancient social concepts. In a speech given during a conference on privacy i 2000, Umberto Eco [31] points on the notion of boundaries that people has used to protect themselves as long as the human race has existed. Walls has been built to keep enemies outside and at the same time keep people and information from getting out. In the case of The Great Wall of China it did defend from invasion of the Celestial Empire, but also kept safe the secret of silk production [31]. There is a theory that the notion of privacy evolved when houses started to include specialized rooms for sleeping and hygienic doings, and it became physically possible to be alone during such activities [32]. Aristotle distinguished between the public sphere of politics and political activities and the private sphere of the family as a private domain for self-regulation and no governmental authority [33]. The respect of privacy grew with the spirit of individualism during the Renaissance and the individual got value where the community up till now had been the dominant unit [32]. In 1890 attorney Samuel D. Warren and Supreme Court Justice Louis Brandeis published the article "*The Right to privacy*" [34] and wrote that *privacy is the right to* *be let alone*. Their focus was on protecting the individuals and they related this to privacy challenges evolving from the development of new technology and gossiping journalism, which are well known challenges in our society today. In particular they referred to the possibility to take photos with a fast camera. Photography war earlier a dreary process where the object had to sit still for a long time to capture the subject.

Essential in our understanding of privacy today is the right to control who has access to information about us, so-called private or personal information [35]. It is primarily this part of privacy that is extensively regulated by laws and will be examined in the next chapter. Misuse of information is also the mostly used argument in the discussion of privacy, and with the exponentially growth of information technology from around 1970, new challenges in regard of privacy has evolved. Privacy is often associated with ICT due to the focus on personal data, but there are more existential values affiliated with it.

Privacy, or to be alone is an important part of interacting with other people. Being alone makes us able to relax, reflect and develop our personality. Surveillance can have the effect that we alter the way we behave, and hence loose our spontaneity. People who restrict their actions because someone might observe them will have less feeling of freedom and individualism, which both are important aspects of the liberal tradition. Some parts of our life can function only when we are totally alone, or more important, when we are absolutely sure that no one observes us [36].

Our apprehension of privacy differs according to time, culture, habits, traditions and social structures, however it seems like all cultures have some conception of privacy and having a private life. Privacy means different things to different people, which causes the term to be multidimensional, complex, context-sensitive and very hard to define [11, 36].

Privacy cannot be understood independently from society because the need for privacy is socially created [4]. Interaction between people, institutions and governments often results in friction and conflicts. Having privacy means that one can retire from this activities and frictions, otherwise individuals would not be able to engage in society the way we do.

Privacy has been topic for cultural and artistic creativity and production for many years, and shows that we regard social issues according to privacy both interesting, entertaining and a little bit frightening. Several world wide known books, films and plays have shed light on challenges around privacy and misuse of personal information. The most obvious and most referred to of all examples is George Orwell's novel *Nineteen Eighty-Four* [37] published in 1949, which refers to a society with omnipresent governmental surveillance and the public is stripped from all form of privacy, even individual thinking. In Charlie Chaplin's film *Modern Times* from 1936 [38] the main character is being subjected to indignities of total surveillance in the factory he works in. The famous play *Hedda Gabler* [39] written and published in 1890 by Henrik Ibsen shows how a power relationship evolves when one person knows compromising information about the other. Judge Brack knows the secret of Hedda giving Løvborg a gun to kill himself, and she says in despair: *I am in your power none the less. Subject to your will and your demands. A slave, a slave then!*

An interesting phenomena in society today is that it seems like more and more people tend to expose themselves and their private life through different media such as social networking sites and apps with little restrictions of what they share. Some see this as a result of gossiping journalism where celebrities frequently participate in sharing information from their private life while others are subjects of the paparazzi. This might contribute to a reduction of our privacy awareness and the boundary between our private and public life fades out [31,32].

The debate of privacy today is highly characterized by the tension between fundamental principles of privacy, where the individual has the right to know and decide who can collect its personal information and to what purpose, and the registration and use of personal information as a tool for fighting crime and terrorism. The resolution of implementing EUs Data Retention Directive [40] and the disclosures of NSAs (National Security Agency) mass surveillance program PRISM [41] are amongst the most commented and discussed cases.

3.2 Privacy challenges

Since the 1970s, computer technology has developed to become an important and widespread tool both in business, education, public institutions, military, finance and numerous other areas in addition to play a leading role in our private lives. As a result of this development, the possibilities to collect, store and use data in different ways, has increased enormously. Since we are dependent of use of personal identification and information in many of the functions in our society, naturally the question of securing our personal information arises. The challenges regarding the protection of personal information are considerable, both technical, legal and related to organizational and human aspects. Absolute security is impossible to achieve and therefore it is necessary to perform risk assessments to decide the level of acceptable risk. For businesses and organizations there must be a balance between sufficient security mechanisms and cost based on the risk assessment [42]. This section will shortly describe some superior categories of important challenges in regard to privacy and smart grid.

Technology

Technology is sometimes mentioned as a threat to privacy, but technology in itself is not what creates privacy problems. One can argue that computers make it possible to steal personal information, but it is the way we use technology and build our systems that can lead to vulnerabilities. Securing information has become a necessary and integrated part of information technology. The goal is to ensure protection of personal information, or in more general term to secure functions of the society, since almost every important information systems has become digitalized.

One way to address privacy challenges in a technological context is to define how we can achieve secure computer systems. The goal is to develop robust and effective information systems which attends to availability and at the same time assures confidentiality and integrity. These demands are also stated in the Personal Data Act 2004-04-14 [10]. There exist slightly different definitions of these terms according to context, but the following are in relation with privacy and personal information.

Availability imply that correct information is accessible and usable by authorized persons upon demand [42,43]. This includes robustness to system malfunction or attacks like Denial of Service (Dos, DDos). It is a lack of security mechanisms to handle problems like DoS, and in some situations strong and restrictive mechanisms might actually lead to a reduced availability [43]. Availability is related to the right to access and correct private information about yourself.

Confidentiality is to make sure that no unauthorized persons get access to specific information. In some situations it might include not only securing the content of an information, but to keep secret the existence of it. The property anonymity is confidentiality of identity and hides who is linked to the information [43].

Integrity imply that no unauthorized changes is made on the information, neither accidental nor malicious [42].

Some may argue that the list is incomplete without the topics authenticity, accountability and non-repudiation [43]. The term authenticity is mentioned as a special case of integrity where the case is to proof that a person or a document is what it claims to be [42]. Accountability is to keep audit information about access and change of information. Non-repudiation provide unforgeable evidence that an action has occurred. To comply with the previously mentioned requirements for a secure computer system, there are both technological and organizational/human challenges.

Legislation

The amount of laws and regulations that affect information security in some way is large and complex. This makes it hard for organizations to have enough knowledge to comply with legislation when they develop and implement digital information services. A survey performed by The Norwegian Information Security Forum (ISF, www.isf.no) shows that there are nearly 40 laws and regulations which hold specific demands for information security in Norway [44].

Privacy is not included in the Norwegian constitution in contrast to for instance freedom of speech. This is unfavourable in cases where there is a question of balance between privacy and other rights. Including privacy as a constitutional right would not change today's legal situation, but it would reinforce the importance of privacy as a human right [45].

Another challenge is the fact that laws and regulations are limited to their area of jurisdiction, but many information services are global, and keeping legislation up to date with the development of networked information systems is a challenge. Unfortunately, among legal scholars there is no common agreement of a universal definition of privacy and attempts to define a set of characteristics or properties has failed [11]. This might lead to a different interpretation of legislation even if the basic laws and regulations documents are the same in several countries. There are several international directives and guidelines which aims to achieve a common baseline and a homogeneous privacy legislation to secure personal information which is transferred between countries. Examples are the European Data Protection Directive and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Legislation in regard of privacy and smart grid will be examined in chapter 4.

Knowledge

Knowledge of information security is by the Norwegian government listed as a major challenge that should be addressed in all levels of the educational system. *NOU 2013:2 Hindre for digital verdiskaping* [44] points out there are too little knowledge of information security and to what degree digital services can represent a threat to security, with both citizens and businesses.

Meld. St. 11 2012-2013 Personvern - utsikter og utfordringer [45] remarks that consent, also in the future, should be the primary basis for optional registration of personal information. But sometimes both people under age and grown ups lack sufficient knowledge to make a qualified consent, and on many occasions parents or guardians must take this decision on behalf of their children.

Research shows that our awareness of privacy differs with the degree of how salient the privacy concerns are made. If we are confronted directly with an assurance that privacy is taken care of, we tend to be more restrictive about divulging our personal information than if the privacy concerns are depressed [46]. This acknowledges the fact that it is a considerably challenge in helping individuals to navigate the complex questions of privacy.

As a mean to counteract negative effects of digitalisation of information systems, the society needs to have knowledge and understanding of existing threats. The NOU 2013:2 report states that current updated information about assessments of threats from the security organizations is necessary [44]. Many businesses and organizations are small and have limited resources when it comes to knowledge and capability to specify secure functions in their IT-systems. Hence they are dependent on the contractors. This report points out the necessity of giving this businesses and organizations support when it comes to knowledge and guidance to make sure their systems comply to legal and technical demands of information security. Also when it comes to readiness to manage the situation when a security incident occurs it is of vital importance to understand threats and vulnerabilities to the systems. Many of today's vulnerabilities in digital systems can be reduced by raising the operators and users knowledge and awareness by building a security culture [44].

3.3 Taxonomy to identify privacy problems

To address a problem it is necessary to understand the essence of it. If we do not have a clear understanding what the problems are, how can we address it in a meaningful way? In this case, we need to have a good comprehension of how and why privacy challenges appears. A clear taxonomy of threats against personal information might also be advantageous to persons who finds themselves in a situation where they have to make a decision about their personal information, which presumably all people experience at some point. As discussed earlier in this chapter, there is a need for increased awareness of privacy as the amount of information registered about private persons grow. Another reason to have a good understanding of privacy problems is during work of protecting privacy. If the problems are not fully understand it will be a difficult task to evaluate the effectiveness of the protection mechanisms.

Daniel J.Solove [4] defines in his article *A taxonomy of privacy* a framework to identify privacy problems in a concrete and comprehensive way. His motivation for creating this framework is to provide a tool for the legal system in USA to come to a better understanding of privacy. Although the US legal system is the target for this framework, it can easily be generalized to all areas where privacy challenges exists.

In this thesis Solove's framework will be used as a model to define and give examples of the privacy challenges in the Smart Grid infrastructure. In this chapter the model will be explained according to Soloves article, and in chapter 4 it will be used to classify vulnerabilities in regard to Smart Grid.

In the attempt to get a more concrete definition of privacy, the framework identifies and organizes specific activities that pose privacy problems. Most of these activities are not inherently problematic or harmful to the persons they affect, and if a person consents to the activities, no harm is done. And if it is declared that a harmful activity has happened, it does not automatically result in a legal redress because countervailing interests might prevail. Some of the activities defined have similar characteristics, but they all diverge from the other activities in the way they might harm privacy. We need to know these differences to get a precise understanding of the challenges. Figure 9 shows the elements of the framework.

3.3.1 The model

The model includes two objects, the data subject and the data holders. The data subject is the person whose personal information is being collected and this is the individual that will be affected by the activities. Data holders are the objects collecting and storing information and can be other people, government or businesses. Data holders are the ones that performs most of the activities in the model which are divided into four groups; (I)Information collection, (II)information processing, (III)information dissemination and (IV)invasion. The arrows in the model shows which way the information flows in regard of the data subject. Invasion differ from the other groups of activities because the progression is towards the subject and does not necessarily involve information at all.

I. Information collection

This group defines two types of activities to collect information; surveillance and interrogation.

Surveillance:
Surveillance is monitoring another individual or a group of individuals. This can be done by visual or audio surveillance. It does not necessarily include recording on some kind of media and eavesdropping or peeping through windows can also be regarded as a kind of surveillance. When surveillance is done continuously it can have problematic effects. Individuals that are monitored can feel anxiety and discomfort and in some cases surveillance can make a person behave differently. When surveillance leads to an imbalance of power that makes people change their behaviours like not engage in politics or use their right to free speech it is referred to as a *chilling effect*. But in some cases an effect from surveillance is wanted, for instance video monitoring in a shop to prevent shoplifting.

Interrogation:
Interrogation is questioning or interviews with the goal to extract information from a person. Interrogation raises several questions in regard to privacy. Due to the fact that interrogation is not relevant in the smart grid context, this activity will not be discussed further.

II. Information processing

Information processing describes actions targeted on the data already collected. The activities include use, storage and manipulation. The processing of information diverges from dissemination because even if the information is transferred to another location it does not result in any

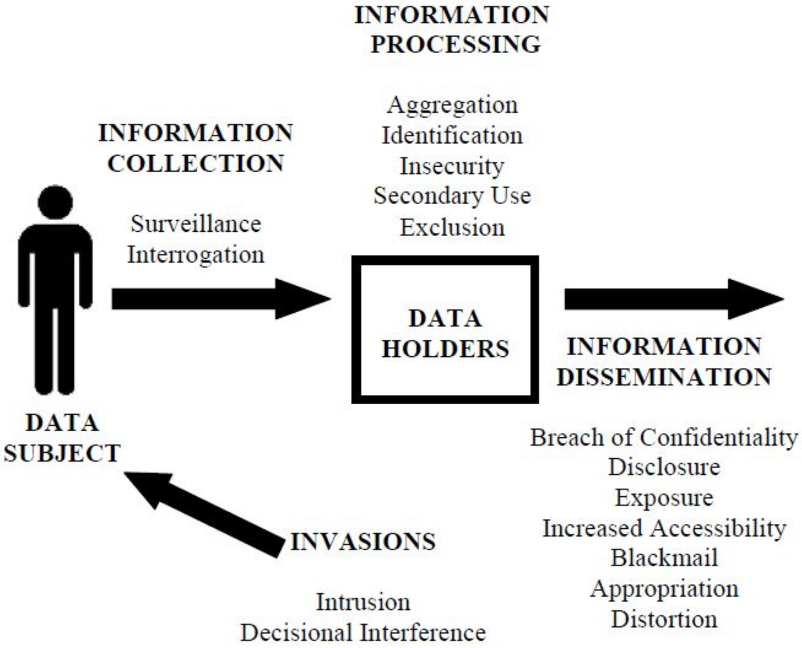

Figure 9: Activities that affect privacy [4]

form of disclosure.

Aggregation:
Aggregation is when already collected data from different sources are combined together and new information is deduced. Aggregation is closely connected to computer technology which is an important tool to even make aggregation possible. Doing such work manually is very demanding, though it is possible to find and combine to pieces of data and interpret to new information. With the use of computers, networks and connected databases the power and scope of aggregation becomes significantly more extensive. And by using state of the art tools for analysing aggregation can result in huge amounts of new information from a relatively small effort. As an example, Google takes advantage of aggregation of information about web-users browsing history and searches to tailor advertisement. Facebook uses the same technique based on among others the users likes and personal information. Aggregation of data can be problematic because it upsets the expectation of what a person think is known about them. We all leave small amounts of information in our daily activities and expects them to be kept separate. These individual pieces might not reveal much about a person, but brought together they can draw an digital picture of a personality, or even worse a wrong picture. Regardless of how much data is aggregated the result will be both incomplete and telling, and information will be disconnected from the context where it was collected. Aggregation differs from the activities listed under information collection because it uses already gathered information and does not include the data subject directly in the activity.

Identification:Identification is the process of connecting a piece of information to a person and makes it possible to verify the identity of someone that claims it. Identification is related to both disclosure and aggregation. It reveals the true identity of a person and links that identity to information. But it differs from aggregation in the way that aggregation does not necessarily connect the information to the person it concerns. Identification has many benefits and while it verify the identity of a person it can also lead to the exposure of an adversary claiming to be someone else. While linking information to persons can have benefits it can also be problematic because information can be baggage. An example from Solove's article [4] describes how a French citizen who had surgically changed her sex from male to female was unable to conceal this because her social security number revealed her sex at birth. As for Norway today the procedure is to issue a new social security number. This example shows that the identification in itself might not be the harm, but the information it connects you to can be a disadvantage.

Insecurity:
Insecurity is when the handling and protection of our data leads to problems. This is illustrated by identity theft. This crime begins with the adversary stealing personal information that is not adequately protected. When this identity is used to for instance purchasing a credit card, the credit card company fails to identify the person correctly. Insecurity exposes individuals to possible future breach of privacy, and one can argue that no harm is done it the insecurity has not lead to any incidents. Many laws and statutes require that information must be kept secure which means that insecurity is recognized as a breach of privacy.

Secondary use:
Secondary use is when information about a person is gathered for one purpose and is later used for another without his knowledge and consent. Solove calls this the purpose specification principle. The motive for using data for another purpose than what was initially the thought vary from benign to malignant. In some cases the information might lead to the prevention of crime or to save lives, but secondary use can cause problems because it opposes what the people expect of the usage of information and is a breach of confidentiality between the data subject and the data holder. If there is a potential secondary use of information given up, people might not share it. Examples of such use is giving out addresses for spam and telemarketing. An important term in this context is consent. If the person gives her consent to secondary use, no harm is done. Unfortunately getting the consent from a person does not remove all problems, because the possible use of data is theoretically infinite and there is a chance that the person does not understand the range of potentially use.

Exclusion:
Exclusion is the failure of giving people information about their records and not providing the possibility to correct or delete the records about him. As with secondary use, exclusion is related to the breach of confidentiality. While the first activity is exposing data to unauthorized parties, exclusion is failing to give an authorized person access. In a society where increasingly more personal information is collected and used to make important decisions it is an important principal of legal protection to give the individuals access to control the data integrity.

III. Information dissemination

Information dissemination is activities where harm is done by revealing personal data or there is a threat of spreading information.

Breach of confidentiality:
Breach of confidentiality differs somewhat from the other activities in this group because it is a direct violation of trust between the data subject and the data holder, and the harm emerges from this violation, not primarily the dissemination of information. In a situation where the data subject and the data holder are in a customer-company relationship the harm might be of greater extent for the data holder due to loss of trust with its customers. A bad reputation can be difficult to rebuild.

Disclosure:
This activity refers to disclosure of private matters that is offensive to the victim and of no public concern. Disclosure is connected to breach of confidentiality, but in this case the harm includes damage to one's reputation caused by disseminated information, not only violation of trust. Fear of disclosure can have an effect on how people behave, for instance inhibit their interaction with other people. In some cases disclosure can threaten a persons security. Victims of stalking and domestic abuse have good reason to keep their living address secret. The amount of harm is also related to the extent of dissemination. Many people disclose secrets to a limited group of friend, but expect the information not to be spread.

Exposure:
Exposure is closely related to disclosure, but differs in that it involves exposing physical or emotional attributes of a person which he finds embarrassing and offensive. Exposure does not actually reveal any new information, but it leads to harm due to social practises we have developed in our society, for instance norms about nudity and bodily functions.

Increased accessibility:
Increased accessibility does not involve any kind of disclosure of secret information, but makes already available information more accessible. There is no breach of confidentiality in this case. Better accessibility is a result of more openness, allowing people to easily access information they seek, but this also makes the information vulnerable to exploitation for marketing and other types of secondary use. In this case there is important to consider the consequences of information made more accessible.

Blackmail:
Blackmail is when a person is threaten to fulfil a blackmailers demands for him not to expose personal information about the victim. The demands often involve paying the blackmailer money. Blackmailing creates an unwanted power relationship between the data subject and the blackmailer where the subject is dominated and controlled. The more people know about others, the more control they can exercise, thus preventing blackmail prevents people to take advantage of knowledge about others.

Appropriation:
Appropriation happens when someone uses another person's identity or property of his personality for beneficial gain. Although the name or a picture of a person is not secret, appropriation can cause privacy harm. It is related to the way an individual wants to present herself to society, and having one's person commercialized without consent can be very humiliating. Solove [4] points out that harm from appropriation comes from interference with freedom and self-development.

Distortion:
Distortion is similar to disclosure because it reveals information to unauthorized people, but in addition the information is manipulated or misleading or wrong. Harm from distortion comes from the victim being exposed to the public in a inaccurately way, which in turn affects the persons reputation. Our reputation is valuable in the way we interact in society, and rebuilding a disrupted reputation can be a difficult task.

IV. Invasion

The last group of activities is called invasion. It differs from the other groups because the information involved is not the most important aspect. The harm comes from the unwanted presence of someone or something monitoring people.

Intrusion:
The right to have a private life and to be let alone in our private homes is one of the fundamental parts in privacy statutes. Intrusion occurs when individuals are disturbed in their private sphere or in their daily activities in a way that makes them feel uncomfortable. Intrusion is often associated with physical invasion and proximity, but surveillance from a distance over time can feel just as invasive. Intrusion can also be of digital character, like intrusive marketing, spam and junk mail.

Decisional interference:
Decisional interference is when the government interferes with peoples decisions regarding sensitive or private matters of their lives. Other activities in this model where harm can result in people changing their actions has similarities with decisional interference, but in this case there is a direct involvement by the government.

Discussion of the model

This taxonomy describes the problems that can arise from breach of privacy in a clear and exhaustive way. Although this model is developed for the legal system to get a better understanding of harms arising from privacy breaches, this knowledge is useful in other situations as well. As mentioned earlier in this chapter, knowledge and awareness when it comes to privacy is a challenge on all levels in the society from system architects to end users. The concept of Privacy by Design (PbD) involve privacy concerns in all stages of a systems life, from planning to closure. The model does not have a technical perspective, but achieving a clear understanding of possible privacy problems is helpful when assessing vulnerabilities in a system and subsequently choosing appropriate technical security mechanisms. For end users this model might be useful to get a better understanding of possible negative consequences of giving up personal information, but also enlighten a users right to access, correct and delete personal information.

4 Legal aspects of privacy and AMS

4.1 Legal aspects

This section will consider and discuss Norwegian privacy legislation with relevance for privacy in AMS and smart grid. European directives and international guidelines which has been influential to Norwegian privacy legislation will also be considered.

According to Jansen and Schartum (2005) [42] there are tree different scenarios where we consider information security; (I) Security of the nation and other vital national security interests, (II) functions that are critical to the society, including security and readiness, and (III) other functions of the society and security of individuals. Security and privacy in smart grid lies within scenario II and III. One of the means to obtain information security in these scenarios is legislation. In addition to the Norwegian constitution, laws and regulations, Norway is obliged as a member of EEA (no: EØS) with the EU. The EU legislation is called regulations which are binding, and directives which the member states must implement in their own legislation according to the directives framework. EU legislation considered in this thesis are directives.

An essential element when we discuss privacy is protection of personal information, and it is primarily this dimension that is extensively regulated by laws. Privacy legislation is not limited to the individuals right to decide who can access their personal information. There are also requirements to the processing of the information, data quality, the right to access data and protection of data. These aspect are covered in the laws, regulations and directives listed in this section.

Some principles are fundamental in our privacy legislation: [47].

- The reason for collecting personal information must be objective and there must be a legitimate and clear purpose.
- Collecting personal information must be based on a well informed consent.
- Data controller is obligated to inform the data subject about purpose, secondary use and whether the registration is mandatory or not.
- The data subject must have access right to his records.
- Information collected must be correct and up to date.
- Incorrect information must be corrected or deleted.
- Unnecessary information which purpose is outdated must be deleted.
- Data controller is responsible for adequate information security and there must exist documentation of security and risk assessments.
- Sensitive information must be subject for increased regulations and security.
- Individuals must be able to roam anonymously if new technology is being used.

- The data subject must have the right to have decisions made manually where the decision making is automated based on collected information.

In the following section important parts, in regard of privacy and smart grid, in the laws, regulations and directives are emphasized.

4.1.1 Directive 95/46/EC

The European Union directive 95/46/EC [48] *Protection of individuals with regard to the processing of personal data and on the free movement of such data* was passed in 1995. The development of information systems has evolved tremendously since then. Despite this, the fundamental privacy principles of the directive is still valid.

As this is a EU directive, the member state of EU or EEA must implement it in their own legislation in a way they find appropriate, but inside the directive framework. The objective of this directive is to apply homogeneous national laws and regulations in all member states in regard to protecting privacy and personal data. A wide variety of national laws and hence differences in the level of protection inhibits the possibility of free movement of personal information between the states. Section 10 in the directive states that this approximation of laws must not result in less protection, but on the contrary ensure a high level of data protection [48]. The directive outlines a minimum, which means that the member states are free to implement higher standards of protection in their legislation. Consequently, the desirable harmonisation of the states laws is not achieved. Because of this fact amongst others, the directive is up for revision in the European Commission. Better harmonisation of legislation and better clarity of the controllers obligations and rights for the data subjects is central elements in the revised draft. For instance the right to have their personal information deleted after the purpose is outdated is central, also known as *the right to be forgotten* [45]. In general the directive is ready to be updated to meet the fast development of technological solutions which handles large amounts of personal data.

The directive is relevant to privacy and smart grid because its framework is mainly implemented in the Norwegian Personal Data Act [10] which is referred to in more detail in the next section.

4.1.2 Personal Data Act and Personal Data Regulation

Personal Data Act LOV-2000-04-14-31 [10] and Personal Data Regulation FOR-2000-12-15-1265 [49] is the main legislation according to protection of personal information in Norway. The Personal Data act implements EU directive 95/46/EU. The purpose of the Act is *to protect natural persons from violation of their right to privacy through the processing of personal data. The Act shall help to ensure that personal data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensure that personal data are of adequate quality* [10]. This implies both that the personal information must be sufficiently protected, but also there is a demand that the data must have good quality to ensure that decisions made on basis of the information is correct and attends to the due process of each individual.

Before further discussion, there is important to have a good knowledge of some of the definitions in this Act (§2).

1. Personal data: any information and assessments that may be linked to a natural person.
2. Processing of personal data: any use of personal data, such as collection, recording, alignment, storage and disclosure or a combination of such uses.
3. Personal data filing system: filing systems, records, etc. where personal data is systematically stored so that information concerning a natural person may be retrieved.
4. Controller: the person who determines the purpose of the processing of personal data and which means are to be used.
5. Processor: the person who processes personal data on behalf of the controller.
6. Data subject: the person to whom personal data may be linked.
7. Consent: any freely given, specific and informed declaration by the data subject to the effect that he or she agrees to the processing of personal data relating to him or her.
8. Sensitive personal data: information relating to
   - racial or ethnic origin, or political opinions, philosophical or religious beliefs,
   - the fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act,
   - health,
   - sex life,
   - trade-union membership.

The scope of the Personal Data Act is (I) processing of personal data wholly or partly by automatic means and (II) other processing of personal data which form part of a personal data filing system. Automatic means in this context is by use of electronic equipment. A third scope (III) is surveillance by camera. This is an example of national legislation being more restrictive than the EU Directive, since camera surveillance is not a part of the scope of Directive 95/46/EC (§1). The territorial extent of the Act applies to controllers who are established in Norway and in other countries (also outside EEA) if the controller makes use of equipment in Norway. This does not apply for equipment used only for transfer of data (§4).

Chapter two lists general rules for processing of personal information, both personal information in general and processing of sensitive information (§§8 and 9). §11 states that the controller must ensure that the personal data is only used for explicitly stated purposes and not used for other purposes subsequently without consent. Further it states that data must be accurate and up-to-date. This reflects the right individuals have to know who has access to their personal data and that there must be a guarantee that the data is not subject for secondary use as long as the owner has not given her consent. §15 enforces the fact that the processor cannot process the personal data in any way other than what is agreed in writing with the controller. This is a chain of consent from the individual to the controller and further to a third-party processor.

§13 deals with information security. The controller and the processor are responsible for a sufficient security through planned and systematic measures with regard to confidentiality, integrity and availability. Security measures and system shall be well documented. If the controller allows other persons to access these data to perform tasks in connection with the system, he must ensure that the security requirements are fulfilled.

Chapter three of the Act deals with the right to information about his personal data. This includes information about the controller, the purpose. origin of the data and secondary use. It also includes information about the security measures, as long as it does not jeopardise the security.

§28 states that the controller can not store data longer than what is necessary for the purpose. If no other law require storage, they must be deleted. An exception is for historic, statistical or scientific purposes.

According to transfer of personal information to other countries. §29 express that data can only be transferred to states which ensures an adequate level of protection, for instance countries which has implemented directive 95/46/EC [48]. There are some exceptions from this paragraph, for instance if the data subject gives his consent.

The Personal Data Regulation expresses the more practical approach to the requirements of information security. It raises demands to the organization of the security management, risk assessments and personnel. It also enforces the requirements of confidentiality, accessibility and integrity.

4.1.3 Energy Act and Energy Regulation

The Energy Acts [50] objective is to ensure that production, redistribution, transfer, trade and use of energy takes place in a rational way according to the society. Privacy and information security of personal information is not a direct topic of this Act since that is met by the Personal Data Act. But some of the paragraphs might have influence on how personal data is processed.

According to §§4-6 and 4-7 there is a demand to difference between the distribution system operator (DSO) on the one side and power production and electricity distribution business and on the other, both legal and functional. The consumers is free to chose whatever electricity distribution company (EDC) they want to purchase their electricity from. This is of importance in regard of access to information about energy usage where both the DSO and the EDC has access to this information.

Section §9-3 deal with information security of system information regarding power distribution. The DSOs must assess what information is sensitive according to the systems, their locations and access of personnel. This type of sensitive information must be restricted and not accessible for unauthorized persons.

The Energy Regulation [27] is up for revision by the Norwegian Water Resources and Energy Directorate (NVE), and the new regulation will be coming into effect January 1st 2019. The changes are made to apply with the coming obliged deployment of advanced metering systems (AMS). The regulation describes the distribution of responsibility and the level of functionality that must exist in the AMS. §§3-1 and 4-1 states that the DSO is responsible for all meters and meter data in their area and they are obliged to install the meters.

Requirement of functionality is described in §4-2. AMS shall:

- store registered values of usage with a frequency of maximum 60 minute and be able to adjust this frequency to 15 minutes,
- have a standardized interface which is prepared to communicate with external equipment based on open standards,
- be able to attach and communicate with other types of meters,
- ensure that registered data is not lost it there is a voltage interruption,
- be able to stop or restrict effect outage,
- be able to send and receive information about pricing and communicate errors,
- be secured against misuse and unauthorized access to managing functions,
- register effect floating in both directions.

Metering data has to be stored in the meters until they have been transferred to the DSO. As described in §4-3 they must be accessible to the user and the EDC at 9.00 AM the next day. §4-4 also states that information about usage must be accessible on Internet in a format where it can be used to compare usage and costs.

According to storage of metering data, DSOs must store data for minimum 3 months and maximum 15 months with a granulation of 60 minutes. Data of monthly granulation has to be stored and accessible for three calendar years.

4.2 International collaboration of privacy legislation

An international collaboration in regard of privacy legislation becomes extensively important as personal information flows across borders. As stated by the OECD Secretary General *personal information is the currency of Internet economy* [11]. There are numerous international arenas for work and collaboration on privacy challenges. This section will list some of the projects where Norway participate or where the results is of importance of Norwegian interests. Several regulations is under ongoing revision as a result of increased use and flow of personal information on the international market.

European Union

According to work on privacy, there are two groups in EU. Article 29 Data Protection Working Party is a collaboration between supervision authorities in the member states, and Article 31 group which is a group on ministry level. Even though Norway is not a member of EU, the Norwegian Data Protection Authority is represented in the Article 29 group [45].

OECD Guidelines

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data is not legally binding for the member states, but have been of great influence of privacy legislation especially outside of Europe. OECD is an important arena for privacy discussions to get common understandings of current and future challenges [45]. The purpose for these guidelines is of equal character as the European directives on privacy: *OECD Member countries considered it necessary to* *develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data* [51]. The work on privacy in OECD is performed by the Working Party on Information Security and Privacy and Norway is represented in this group. The task of revising and updating the guidelines was started in 2010

Council of Europe

The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was passed in 1981 and is implemented in the Personal Data Act. The convention was worked out to reconcile fundamental values of the respect of privacy and free flow of information between people. This document is outdated in regard of the technological development that has been going on since [52]. This convention is up for revision and Norway is represented in this work.

5 Privacy vulnerabilities and threats in AMS/Smart grid

Privacy vulnerabilities in the AMS and its infrastructure is the result of the functionality of the smart meters and the transmission of fine grained data to the utility companies' systems for storage, invoicing and grid management. As discussed in chapter 2 these data can reveal information about when people living in the house with AMS meters are at home or not, their activities and habits. The scope of this thesis is the privacy aspect of AMS and will not present a comprehensive list of threats in regard of information security. This chapter shortly discuss several threats that can affect the customers privacy and what problems they can cause by compromising the personal information and data from energy usage. It also briefly presents the concept of Privacy by Design (PbD).

5.1 Overview of threats and vulnerabilities in the AMS infrastructure

General threats to computer and information systems can be divided in three categories; (i) unintended or accidental threats, (ii) general attacks and (iii) targeted attacks [21].

Unintended errors are incidents like natural disasters, hardware crash or human errors.

General attacks are attack targeting IT-systems in general, not one particular system or unit. Examples are malware (viruses, trojan horses, worms, spy-ware, key-loggers etc.) or tools for automated attacks like DDoS.

Targeted attacks are attacks directly on IT equipment via internet. Both general and targeted attacks can be performed by internal or external adversaries.

The following threats are from all three categories mentioned above, and represent vulnerabilities in regard of privacy in the AMS infrastructure.

5.1.1 Communication channel

To enable the communication between the smart meters and the HES, communication channels must be deployed between the utility companies and the metering points, also known as the smart communication subsystem [5]. There are no standard choice of technology when it comes to communication, and the security level of this part of the subsystem might vary depending on what technologies are chosen. There is a possibility that the system for end-to-end communication in AMS will consist of a mix of different technologies combined to deploy a channel where security is handled with different mechanisms and different security levels. It can consist of both wired and wireless technologies. Examples of wireless technologies are wireless mesh networks, cellular communication, cognitive radio, IEEE 802.15, satellite communication and microwave or free space optical communication. Wired technologies that might be used are fiber optic and powerline communication [5]. Every one of these technologies have different situations where they are more suitable due to their qualities.

According to privacy, information leakage and data manipulation or false data injection is the main groups of threats to privacy in the wireless communication channel [53].

Information leakage is when an adversary monitors the communication channel and extracts data transmitted over the media [53] (Confidentiality).

False data injection or tampering compromises the data integrity by inserting false or manipulated data into the system [53, 54] (Integrity).

Privacy problems that can arise from these threats are first of all surveillance which compromises the confidentiality. By monitoring the channel, an adversary can collect data from a smart meter over a period and deduce the in house activities. After collecting the data, there is a possibility of secondary use or disclosure of the information, or aggregation with data from other sources to make an even more detailed profile of the customers activities. Based on where in the infrastructure the monitoring is done, data from one or several meters passes through the channel.

Mechanisms to address the vulnerability of information leakage in the communication channel is mechanisms like encryption [28, 53] and anonymization of data [8] to secure that data cannot be connected to an identifiable person. Privacy is also about securing the correctness of data, and false data injection is a threat to the data integrity. To ensure that false data are not injected into the system, mechanisms for authentication must be implemented, both to ensure authenticity of the parties in the communication, and that the data are genuine [55].

5.1.2 Smart meters

A vital part of the AMS and smart grid is the smart meter which monitors the electricity in the metering point and communicates this information with head end systems (HES) in the utility company's operational center. The smart meter is the physical point of contact between the DSO and the customers, and is a vulnerable element in regard of privacy in the AMS infrastructure. A smart meter can be subject for attacks on both confidentiality, integrity and non-repudiation [56].

Spoofing is to pose as another identity. For instance an adversary posing as a master meter or another node in the infrastructure to trick the smart meter to send data [3] (Authenitcation and confidentiality).

Tampering is when new messages or manipulated messages are sent to the recipient. The source can be both compromised meters or adversaries posing as a meter [3] (Integrity).

Information leakage might be a result of compromised meters sending information to unauthorized parties. If data is exchanged between a smart meter and third-party-device, there will also be a question of security level of the external device (Confidentiality).

Repudiation threats is when one of the parties in the AMS communication channel can deny receiving a message. Non-repudiation or accountability is important due to financial and billing purposes and to ensure integrity of personal information [3] (Accountability).

Choke switch is a functionality of the smart meter which makes it possible to reduce or stop electricity outlet at the metering point. This functionality might be used to reduce outlet in cases where the customers have payment problems. In a privacy context, this is an intrusive act to the household, and it is an important question to discuss who should have the authority to perform this action. The switch is also a possible target for adversaries if the smart meter or the DSO control system is compromised.

Leakage of personal information might result in surveillance and disclosure, and subsequently in secondary use and disclosure. The risk assessment of AMI in Demo Steinkjer [3] notes that the HES and other systems of the DSO becomes more exposed to attacks when connected through the networked infrastructure.

To address these threats, means must be taken to secure the meters both physically and technological to ensure integrity and confidentiality of data and authentication of the communicating parties [56].

5.1.3 Nodes/Master meters

Some smart meters (slave meters) might not communicate directly with the DSO, but via master meters that functions as nodes with direct communication to the DSO. The threats to these meters are in many ways the same as for slave meters, but the consequences might be more severe due to leakage of personal information since the amount of accessible data passing through are larger.

5.1.4 Distribution System Operator

Control systems are extensively used by DSOs in electric grids, and all information being communicated in AMS makes the foundation of the smartness of the grid. Therefore the systems at the utility companies aggregate large amounts of metering data from energy consumers to be used both for correct measuring of energy usage and billing purposes and for analysis, planning and management of grid operations. These systems are targets of adversaries as commercial off-the-shelf information technology products integrates with or replaces proprietary systems. Well known attacks on computer systems as break-ins, industrial espionage and malware attacks will among others be highly relevant for the power industry [57]. Threats to the systems can be categorized as internal or external.

Internal threats are threats originating from inside the DSOs systems. They can be intentional or accidental. Intentional threats can be initiated by disloyal employees that has access to systems or personal information and leads to breach of confidentiality. There are also a risk of unintentional incidents where persons accidentally or without better knowledge disclose private information.

External threats are for instance attacks from adversaries targeted directly to components or systems in the AMI. Through integration of ICT and existing control systems, new threats known for the ICT domain are introduced to the energy industry.

Technical measures must be taken to achieve a security level where the risk is evaluated as affordable. Strict systems for access control and accountability must be implemented to hinder intentional or accidental access and disclosure of personal information. Security mechanisms as firewalls and IDS/IPS [58] and routines for security updates should be implemented as means to minimize the risk of attacks.

But information security is also about knowledge and awareness. The change from proprietary systems to modern information technology results in a gap of knowledge [57]. Prior to AMS deployment it should be taken measures to raise knowledge, prepare for incidents and build further on the existing security cultures to ensure proper handling of data.

5.1.5 Central hub

With an implementation of a central hub for storage of all information about electricity customers, the security of this hub is of considerable importance for customers privacy. There are no implemented solution for Norwegian electricity data yet, but there is an ongoing work to assess a possible common solution with the Danish company Energinet.dk [20].

Although there are no implemented solution, threats to this system will be of the same fashion as to DSO control systems, Both internal and external. In addition, there is the aspect of availability of the information to the customers. A data hub might be a target of DDoS (Distributed Denial of Service) attacks which results in the service being unavailable during the attack.

5.1.6 Non-Utility Service Providers

Non-utility Service Providers (NUSP) is not a main element of the AMS infrastructure, but might consist of components or services that handles personal information about energy usage and hence it is natural to mention this aspect of SG. As described in chapter 2, NUSPs offers products and services independent of the utility companies with the use of data from energy usage. Making these data more available makes it more vulnerable for leakage of personal information. Privacy concerns includes for instance exposure of customer behaviour pattern for commercial purposes and monitoring of customer activities in the homes. In contrast to DSOs which is under strict regulation, NUSPs are not regulated in the same way, and if data is transmitted to services outside Norway, we have little control of what legislation is applicable or how this data is managed and secured.

5.1.7 Non-Intrusive Load Monitoring

In the preceding example of data analysis in chapter 2, data of hourly measurement of electricity usage was analysed. Electric meters can also have the functionality of measuring current and voltage for analysing and deducing what appliances are used in the house as well as their individual energy consumption. This technology is called Non-intrusive Appliance Load Monitoring (NALM) or Non-Intrusive Load Monitoring (NILM). A non-intrusive appliance load monitor monitors an electrical circuit with several appliances and uses sophisticated methods with analysis of the current and voltage of the total load to find information of energy consumption of the unique devices [59]. This represents a threat to privacy of individuals living in the household, as illustrated in the article by E.L.Quinn [9].

5.1.8 Summary of AMS privacy threats and vulnerabilities

Table 2 summaries the threats discussed in this chapter together with the problems it can cause for privacy in AMS. Due to transmission of smart meter data, every part of the AMS infrastructure is vulnerable in regard of privacy problems. Countermeasures consists of both technical and organizational means. The fact that proprietary systems melts together with modern information technology also raises challenges according to knowledge and security culture. It is a presumption that the actors involved in deployment of AMS acts on these challenges to ensure that privacy are not neglected.

Infrastructure	**Threat**	**Privacy concerns**	**Countermeasure**
Smart meter Master meter	- Tampering - Spoofing - Information leakage - Repudiation - Unauthorized or unintended use of choke/switch	- Surveillance - Disclosure - Aggregation - Secondary use - Distortion - Intrusion	- Tamper resistance - Physical security - Authentication - Enciphering
Communication channel	- Information leakage - False data injection	- Surveillance - Disclosure - Secondary use - Aggregation - Distortion	- Enciphering - Anonymization - Authentication
Utility company	- Snooping - Attacks on control systems/databases - Information leakage	- Breach of confidentiality - Disclosure - Secondary use - Aggregation - Identification	- Access control - Accountability - IDS/IPS - Firewall - Physical security
Central hub	- Break-ins - DDoS - Information leakage	- Breach of confidentiality - Disclosure - Secondary use - Aggregation - Exclusion	- Access control - Accountability - IDS/IPS - Firewall - Physical security

Table 2: Privacy concerns in Advanced Meter Infrastructure (AMI)

5.2 Privacy by Design

Privacy by Design (PbD) has become a worldwide standard for designing protections and is recognized as *an essential component of fundamental privacy protection* [60, 61]. PbD involves that privacy and data protection are embedded in all parts of development and application of information technology. In cases where privacy settings are flexible, the default settings should be the most restrictive in regard of privacy. This means that the user must take an active choice to change these setting to less restrictive. This is a proactive way of thinking of securing personal information, and despite PbD has been an important target for international actors for several years, Norwegian businesses and organizations has not yet fully adopted these principles, and PbD is not required by law.

Privacy enhancing technologies (PETs) are technological solutions to secure personal information in existing solutions. An example is "Do-not-track" which is a technological standard which aims to obstruct tracking in web surfing [45]. A system build on the PbD principles should not, by definition, result in any need of PETs since privacy is taken care of in the system. In the Working paper from the International Working Group on Data Protection in Telecommunication [61] there are recommendations for smart metering initiatives, based on best Practices for Privacy in the smart grid [62].

- Smart metering initiatives should feature privacy principles in the overall project governance framework and proactively embed privacy requirements into their design, in order to prevent privacy-invasive events from arising.
- Smart meters should ideally protect privacy by default, with no action required on the part of the consumer.
- Privacy should be an essential design feature of smart meter systems and practices.
- Smart metering initiatives should avoid unnecessary trade-off between privacy and other legitimate functionalities or organizational objectives.
- Privacy and data security should be maintained end-to-end – full lifecycle protection.
- Smart metering initiatives should be visible and transparent, and should utilize accountable business practices; consumers should be assured that the technology operates in accordance with stated objectives.
- Smart metering initiatives should be designed to respect consumer privacy – keep it user-centric.
- Regulatory frameworks should foster the introduction and use of privacy-friendly smart meter and smart grid applications.

5.3 Privacy policies

A factor to obtain a successful deployment of AMS is communication with the customers [2]. As a part of the communication, the companies privacy policies are important ingredients. A privacy policy disclosure are signals to the customers about how they deal with personal information and are important tools in building trust and relationships with electricity users [63]. The work of preparing a privacy policy is also a reflecting process where evaluating the companies policies might help see from a different angle and disclose weaknesses in how the company handles privacy.

6 Methodology

This chapter describes the methods chosen as a tool to answer the research questions of this thesis. It also summaries the arguments for why the respective methods was chosen.

6.1 Choice of methods

While choosing research method one must start off by finding the most suitable approach for the research, qualitative or quantitative approach. Quantitative research is used to answer questions where the researcher aims to find the relationship between measured variables and the analysis is based on statistical methods.

Question	Quantitative	Qualitative
What is the purpose of the research?	- To explain and predict - To confirm and validate - To test theory	- To describe and explain - To explore and interpret - To build theory
What is the nature of the research process	- Focused - Known variables - Established guidelines - Predetermines methods - Somewhat context-free - Detached view	- Holistic - Unknown variable - Flexible guidelines - Emergent methods - Context-bound - Personal view
What are the data like, and how are they collected?	- Numeric data - Representative, large samples - Standardized instruments	- Textual and/or image-based data - Informative, small samples - Loosely structured or non standardized observations and interviews
How are data analysed to determine their meaning?	- Statistical analysis - Stress on objectivity - Deductive reasoning	- Search for themes and categories - Acknowledgement that analysis is subjective and potentially biased - Inductive reasoning
How are the findings communicated?	- Numbers - Statistics, aggregated data - Formal voice, scientific style	- Words - Narrative, individual quotes

Table 3: Quantitative and qualitative approach [6]

The purpose of quantitative research is to explain, predict and to control phenomena. Qualitative approach is to used to answer questions about the complex nature of phenomena and to be able to describe and understand them [6]. Table 3 lists characteristics in qualitative and quantitative approaches. The purpose of this thesis is to get a better understanding of the situation evolving from the deployment of smart grid in regard of privacy challenges, hence the qualitative is the approach of choice in this project, and following are the arguments for this conclusion;

The purpose of the project is to get a better understanding of a complex situation rather than trying to explain and predict. The process will be more holistic and emergent than typical quantitative methods, and it aims to get a better understanding of the situation by interacting with participants. Data that will be collected in this project are not divided in discrete measurable variable, but collected in for instance loosely structured interviews with people with knowledge and skills. Data collected will not be subject of statistical analysis, but rather a subjective analysis with use of inductive reasoning. The result is hopefully to capture the complexity of the situation and to illuminate the problem for discussion and subsequently draw some theories about how these challenges should be handled.

In the qualitative approach there are several designs according to Leedy and Ormrod (2005) [6]; Case study, ethnography, phenomenological study, grounded theory and content analysis. In this thesis case study with interviews and data analysis will be used in addition to a literature study of related work and theory.

6.1.1 Case study

The purpose of a case study is to understand a small number of situations in great depth. In this thesis, interviews is the chosen method for data collection in the case study to make a verbal description or portrait of the cases.

Semi structured interviews

As a case study method to collect data, qualitative semi structured interviews has been chosen. The qualitative interview aims to achieve knowledge as words and descriptions of the situation and not as numbers. The transcription of the interview makes the basis for further analysis.

The questions must have an open design and function more as an initiative to a conversation than a strict questionnaire. It is often better to use short and simple questions and to follow up with more detailed ones.

The interviewer should have good knowledge of the topic, hence a challenge for the interviewer is to maintain a neutral attitude during the interview, not put words in the mouth of the person and keep reactions to oneself [6, 64].

Kvale and Brinkman (2009) [64] lists seven phases of the qualitative research interview:

- Choosing the theme of the interview project.
- Planning and design, including the design of the questions.
- The interview.
- Transcription of the interview.

- Analysis of collected data.
- Verification, is it possible to draw general conclusions, reliability and validity.
- Writing the report.

Data analysis

To describe the nature of data from smart meters, a case of analysing this data will give an visual and descriptive presentation of the data's characteristics.

6.1.2 Literature study

Literature study is a method to get an overview of related work and research and the theoretical background of the topic. The result of a literature study is a discussion with a critical view on related work, and the purpose of this is to give the researcher and the reader a solid theoretical understanding of the current situation. Review of previous work does not give new information to the thesis, but the goal is to give a foundation to understand the current situation in order to conduct a critical analysis and present new theories based on own research.

6.2 Method description

6.2.1 Research question 1

What are the privacy challenges in AMS and smart grid?

As mentioned in the chapter of introduction, there are many sources of research that addresses privacy challenges in smart grid, but they often use the term privacy as an umbrella term with no detailed description of what types of harm the solutions are addressing. This research question aims to answer on a more detailed level what the privacy challenges are in smart grid by using models for taxonomy of privacy. A literature study of previous work on privacy combined with an analysis of the smart grid infrastructure is the most suitable method to answer this question.

6.2.2 Research question 2

How is privacy addressed by the Distribution System Operators (DSO)?

To answer this research question a case study with interviews of representatives from distribution system operators is needed to achieve information for further analysis. The persons to be interviewed must have sufficient knowledge of the process of smart grid deployment in their area of distribution. The interviews will be semi structured with main questions as guidelines for the themes.

6.2.3 Research question 3

What data is captured, transferred and stored by smart meters and smart grid infrastructure related to electricity usage, and can these data be used or misused to deduce information in a format that it threatens the privacy of the consumers?

To answer this question, a case study with data analysis of smart meter data will be used. The result from the analysis will show if information of the household activities can be deduced.

6.2.4 Research question 4

The development of smart grid will increase during the next years, and new applications might find commercial use of the opportunities that evolve from this. How can the society be prepared to handle future privacy challenges arising from smart grid?

The answer to this research question will be of some predicting character, since the deadline for deployment of AMS in Norway is postponed to 2019. In order to answer this question the method will be to study literature of research about possible use and third-party solutions in combination with data from the interviews.

7 Interviews

This chapter describes the process of performing the interview project and the results. There were carried out five interviews with representatives from five different Distribution System Operators (DSO). They all hold positions of project manager or project owner of the DSO's AMS project.

7.1 Interview project

This section describes the phases of the process of performing the interviews in accordance with chapter 6.

Choosing the theme

The theme of the interview originates from the research questions in chapter 1. In order to answer the question about how the DSOs addresses privacy challenges in AMS the questions in the interviews reflect this. The main topics of the interview were; Status of the AMS deployment, how the companies address privacy challenges internal and external, internal routines and security culture and future use of AMS data.

Planning and design

The planning phase includes designing the questions and schedule appointments to carry out the interview. The questions were designed with the purpose of finding out how privacy challenges are or will be handled by the DSOs. The preparing phase in regard of this was to acquire knowledge of privacy, smart grid and how privacy challenges arises from the deployment of the new infrastructure. The selection of participants to this project turned out to be more challenging than expected. Originally the goal was to interview objects representative to the group of DSOs in Norway, but it soon drifted over to just finding persons who was positive to participation. This will be subject for more discussion in chapter 8.

The interview

The main questions, listed in appendix A, were sent to the participants a few days ahead of the interview to give them the opportunity to prepare their answers. The interviews was carried out by telephone in an informal way without strict limitations of the topics of the conversation or time.

Transcription

Transcription was performed during the interview. Since a big amount of information comes up in such interviews, the transcripts was completed after the interview and a report was sent to the participants to let them check for correctness and to give them the opportunity to fill in more information.

Analysing results

By analysing the result, the objective is to find similarities and differences in how the privacy challenges are addressed. We also hope to find out the nature of the challenges existing in this phase of deployment.

Verification

Verification of the results of the interview project is to inspect possibilities to draw general conclusions from the findings. It also includes evaluating the reliability (correctness of the findings) and validity (does the project answer the questions it is intended to answer?) of the findings.

Writing the report

Writing the repost consisted of formulating the findings in a readable and informal format which complies with the ethics of this type of research.

7.2 Results

This section is the documentation of results from the interviews. Transcript from each interview was sent back to the respondent for quality check. Some small changes was made, and some of the respondent added some more information that did not come up during the interview sessions. These results will be subject for discussion in chapter 8.

7.2.1 Case study: Eidsiva Energi Nett AS

Status of AMS deployment

Eidsiva Energi Nett AS has about 140000 traditional meters installed at this moment, and expects to expand this number to approximately 150000 due to development towards point of implementation. They have not decided on technical solutions for the AMS infrastructure at this point but are in the process of evaluating offers. The acquisition is divided in two; one for the meter data system, which is the core system for processing and transmission of data, and AMS technology, which consists of meters, communication technology and the central system (central and distributed technology). Installation services will be purchased from Eidsiva Anlegg, a company from the same corporation, but as mentioned earlier, technology will be purchased form external contractors.

Existing systems are based on proprietary technology, but the new solutions for AMS infrastructure are increasingly founded on open standards. The contractors will base their delivery on their own solutions and/or solutions from sub contractors. The company has decided that they are not willing to take the risk of putting together the infrastructure on their own.

When the company was planning the process of acquisition, they got indications that a solution where the whole process of data collection was outsourced to a third-party might be problematic in regard of security and privacy.

Privacy challenges

The authorities has a strong focus on the privacy aspect in AMS. The company have been involved in the dialogue in the industry and Energi Norge, which is a non-profit industry organization, to get insight in what is the demands in regard of this. The *Guide for processing of personal data in connection with AMS within the energy sector* (AMS guide) [65] offer guidance, but there are still several problems it does not answer. Also other guides and legislation as the AMS Regulation [27] and the Contingency Regulation [66] regulates how they deal with this topic.

During the process of acquisition of new systems for AMS the company have focused on establishing good routines for deleting data, authentication of different users and auditing. The company has two distinctive systems, one for collection and validation of meter data and another for customer information and invoicing. The key to link meter data with customers is the meter-ID. The reason for doing this is to be able to use this data in analysis and at the same time provide some kind of anonymity of the meter data. The Data Protection Authority has been unclear about this solution.

Eidsiva Energi Nett has in their specification for the new systems defined requirements according to privacy and security, for instance enciphering, deleting mechanisms and demands to contractors to handle privacy and their access to data in a secure manner. Some of the requirements from guides can be quite hard to achieve especially for old and distributed technology. This can affect end-to-end security in the total system.

They attend to establish roles according to security organisation and routines in regard of the Personal Data Act [10] when designing their new organisation of operations.

In regard of how the company communicates privacy challenges towards their customers, they act according to the Personal Data Act [10], and implies that the The Data Protection Authority might be of the opinion that the energy business lag behind in regard of this topic. It is unsure if it is possible to include in the contract with the customer in regards of storing data for the purpose of operation and development of the power grid, but the aim is to be able to deliver a service of better quality and stability. The customers cannot decline having a meter installed, but it is unsettled if a new contract is needed or not. The contract is based on a monopoly and the DSOs are very strict regulated.

The company is not familiar to the term privacy-by-design, but they practise this in the way that they consider privacy in the acquisitions, evaluations, through access for contractors, routines and processing of data. They try to do their best, but privacy it is a new area to master in this business.

The most severe challenges in regard of privacy is the possibilities to store data for operational benefits and at the same time maintain privacy and security. It is also a challenge to clarify what is needed of contractual agreements to document the use of this data and the customers consent.

Internal routines

The company is working on implementing routines to make data available to the customers and mechanisms for deleting outdated data in their new operational environment as well as adjusting to guides and legislation. This work is not finished but will be completed with the implementing of the new operational organization. Also routines for auditing, detection of security breaches and contingency will be implemented pursuant to security guides.

According to internal security work the company performs risk assessments prior to the implementation and this will be repeated shortly after implementation. As a result of this they have chosen not to have a physical connection between AMS and the control systems. Switches on the smart meters are therefore not connected to the control system, and a functionality for mass disconnection is not desirable due to security and risk. One of the challenges in AMS is the threat of meters being disconnected unintentionally. Mechanisms to secure communication and hinder adversaries has been a focus in the company's system specification.

They attend to internal security according to The Contingency Regulation [66].

Future use of AMS data

Future use of AMS data is related to the positive effects from use of data in operation, planning and future investments in combination with the dialogue with customers. The biggest challenges is to maintain the security of all this data and at the same time fetch positive effects.

In the AMS Regultaion [27] NVE regulates the periods of storing data of different frequencies. The industry wishes for a longer period, up to 3-5 years storage of hourly measurements to be able to analyse this data in combination with meteorological data. Up until now they have only known usage on aggregated points, but this new data from AMS can be useful for the company's operation. The company fear loss of possible positive effects of the AMS investment if this benefit cannot be collected to make a more efficient operation, better planning and investments and a service of better quality to the customers. A sufficiently long time of storage of data connected to energy usage is vital in this discussion because they want to analyse variations over several years.

7.2.2 Case study: NTE Nett AS

Status of AMS deployment

NTE Nett AS has about 80000 traditional meters installed in their area. As an important part of the planning phase the company has rolled out a area for testing AMS technology, Demo Steinkjer. The project Demo Steinkjer is a national project which is owned by the NTE corporation, and the technical responsibility is placed with NTE Nett AS. NTE Nett builds the infrastructure in the test area, and it functions as a live laboratory where other actors can test solutions which can be commercialized. Both national and international actors take use of this project. The company has implemented 830 AMS meters in Demo Steinkjer. The company expects that the final deployment of AMS and major implementation will occur in 2016 and the year to follow. They are currently in the process of defining system specifications. The biggest challenge in this phase is to decide the level of security. The risk is that the security level in the specifications is too high for any contractor to deliver a solution that comply.

The company has employees with special qualification in regard of information security and telecommunication in relation to both the AMS project and Demo Steinkjer.

Since they have not chosen the technical solutions yet, the Demo Steinkjer project becomes very important as an arena to try out different solutions which is of interest in the final implementation. One of the challenges related to this is that the term information security is too vaguely described in the legislation. Elements that is under testing is security mechanisms and effective and secure communication technologies in the infrastructure. They wish to have a good foundation of knowledge before making decisions in such an important and big investment (250 millions NOK). The test area offers knowledge which is unachievable from a paper analysis. AMS meters are somewhat out of the box products which might be certified, but there are no certification for the whole system end-to-end according to security or privacy. The industry is highly segmented when it comes to products for end-to-end AMS systems. The security aspect is challenging according to continuous security throughout the system, because different technologies have different ways of handling security. What the chosen strategy will be for final implementation is unclear at this point. There are no detailed descriptions of requirements from the directorate (NVE) on this.

Privacy challenges

The company work on privacy challenges in AMS primarily through their mandate in Demo Steinkjer and they have expertise on information security working on these challenges through tests in the demo area. They have a project in cooperation with SINTEF which is called DeVID [1]. The purpose of this project is to perform a risk assessment of privacy in AMS to test hypotheses of how privacy is handled in AMS in regard of selected functions.

When it comes to communication if privacy concerns to customers, the company has decided to await this until the questions around privacy in AMS has been clarified. Customers in the test area are informed about the project, but information to all customers must be awaited to make sure there will not result in a negative effect. Information must be given in the right form at the right time. At this moment there are too many unanswered questions in regard of privacy and security. This is important even though there are no alternative to refuse implementation of new meters for customers in Norway since it is demanded by law. The only way that can happen is if a customer has medical declaration of sensitivity to electricity. A good communication with all customers is important, but it is up to each DSO to make this strategy on their own.

The respondent says Privacy by Design (PbD) is not a term they have implemented as a strategy, but refers to security manager for more information. The work around testing is focused on functionality at this point and the overall picture of information is complex. He assumes this and other terms regarding privacy and security will settle when more of the open questions are answered.

One of the main challenges when it comes to privacy is technical security of the switch in the meter to disconnect power. Hacking is considered as a constant threat and hackers are well organised, hence securing the switch and hinder manipulation of meters is important. There has been tests in Demo Steinkjer on breaking in to the communication channels, but the company has no other experiences in this area. The meters are small computers with two-way communication, and there are many opportunities to control the power in the house, for instance reducing the power for customers with payment problems. The challenge is to protect the individuals with existence of such technical possibilities. The respondent exemplifies a situation where an old women gets the power disconnected and is lying sick and cannot alert anyone. Or a family with small children and little resources that has problems paying the bill.

There is a legal dilemma in implementing AMS because the contract with the customer is based on estimated measurements, and according to that hourly measurements is illegal. But the Energy Regulation [27] regulates the DSO's right to measure energy usage. The question is therefore the necessity of new contracts. NVE and the Norwegian Data Protection Authority are cur-

[1] http://www.sintef.no/Projectweb/DeVID/

rently working on this problem.

Internal routines

When it comes to customers access to their meter data, they are made available through a web portal. Routines for deleting data are established according to the controller role in the Personal Data Act [10] and the contract with the customer. The company has experienced an incident of breach on security routines for processing personal information, and acknowledge that their routines of processing personal information is not good enough.

In the company's view, the AMS Regulation [27] makes the situation impossible in regard of collecting positive effects from meter data, including planning, operation and development. The DSO needs to be able to benefit from the big investment the AMS project is for the companies. To get a useful effect from this data, they need to store data of hourly measurements for 10 years.

Every incident according to privacy and security are reported to the contingency coordinator. Routines for auditing in the new AMS system is connected to testing of communication technologies. For instance by using TCP/IP there will be possibilities for using standardized software to audit abnormalities. The internal security culture in the company has a potential of getting better on the aspect of privacy.

Future use of AMS data

AMS data has a potential of being used in an effective way according to dimensioning of the power grid. There are also possibilities in controlling the energy usage in the households in a better way, but primarily the data has potential in the work of managing the grid.

The biggest challenges in this situation is the amount of data collected and the risk of this information to get away. Third-party misuse by commercialising and exploit is also a threat, for instance hackers steeling data and selling information about whether a person is at home or not.

7.2.3 Case study: Fredrikstad Energi Nett AS

Status of AMS deployment

Fredrikstad Energi Nett AS serves 90000 subscribers. The company operates the demo project Smart Energy Hvaler, a collaboration project between Fredrikstad Energi AS, Hvaler county and NCE Smart Energy Markets, with 8000 smart meters installed in 2011. The company's strategy is to get experiences from this demo project to use in planning for the total implementation. They will await acquisition of technology for the total deployment to get as much knowledge as possible before making final decisions. What technology that will be chosen is an open question at this moment, the communication technology can be either radio, PLC or other. Final deployment is expected in Q2 2018.

The business system is outside their acquisition of the AMS system. There will be considerable changes in information technology to utilize the capacity in AMS. For instance support system for deployment, transfer of orders to electricians with sufficient information and so on. And this must be an automated task flow between internal systems to workers with mobile equipments. The system of collecting and processing meter data is also outside of their AMS technology project, but it is a requirement that it communicates with both the business system and the central hub.

The company is in the process of developing a new system to handle the big amount of meter data, eSmart (eSmart Systems), and the goal is to implement this system before purchasing smart meters, hopefully in mid 2016. Including alarms and sensor data the amount of meter data is huge and they want to implement a system to gain positive effects from analysing this data.

Privacy challenges

The company does not have any initiative on privacy challenges. They attend to discussions and groups in the industry, for instance Energi Norge, where questions in regard of this topic are discussed. Through Smart Energy Hvaler the DeVID project [2] has performed a risk assessment of privacy and information security earlier this year.

Meter data which is used in approved research in demo project is anonymized. No customer information is connected to that data. The only identifiable properties are type of installation (house, cabin, industry), timestamp and value.

The company has not taken any initiative in regard of communication with customers about privacy concerns yet. They have not, in contrast to Demo Steinkjer, obtained consent from the customers in their demo project. All customers in the defined demo area has got a smart meter installed, but the company has not received any complains about this. As mentioned earlier, the data are anonymized when used in research, and in cases of more detailed data, the customers are asked before participation. The process of obtaining consent before the demo deployment might have resulted in reduced participation which they saw as an unwanted situation. The company is very careful when it comes to distribution of this data. Preferably a group representing the customers should have been more involved in the demo project to ensure communication and acceptance in questions of security and privacy. Questions concerning this must be well clarified before implementation to ensure a norm for the industry.

An unfavourable focus in regard of privacy will be very negative for the whole AMS project. From the company's view it is desirable that the directorate (NVE) and the Norwegian Data Protection Authority are more clear in their definitions and requirements in their guides and regulations. Usage of meter data in operations of the power grid is not formulated as a purpose anywhere, and the legislation from the ministries is ambiguous since there is a conflict between use of data for a more effective grid management and only using the data for invoice purpose.

Privacy by Design is not a strategy the company has implemented. They have no self initiated projects on privacy.

The most severe challenges in unintended distribution of meter data to commercial actors and adversaries. AMS data can reveal much information about the customer and it is critical to ensure sufficient security of data and infrastructure since data in AMS has much bigger value than meter data today. An employee has access to much information, and unfaithful employees might present a threat in the AMS infrastructure.

Internal routines

According to internal routines for access to data, this is taken care of through a web portal. The need for this service might disappear from the DSO's responsibility with the implementation of

[2] http://www.sintef.no/Projectweb/DeVID/

a central hub. The situation today is 150 different solution, one for each DSO, and the security is maybe not optimal in all solutions. One centralized solution might be more expedient when it comes to securing the application.

In regard of contingency and security breach detection there has been more focus on functionality than privacy. The company applies to the Contingency Regulation [66] and has documented good results from inspections. The meter switch for reduction or disconnection is an unsettled topic. In the company's customer service, one person has access to this function, but mass disconnection of many smart meters is not possible. It is possible though by using scripts, and this is considered as a vulnerability. This function is actually not a wanted functionality. In reality it is a function to handle customers with payment problems, not a tool to control power supply. It is advantageous in one situation, when electricians does not have to go into peoples homes to disconnect the power due to missing payments, which represent an uncomfortable situation for both parties. But this switch makes hacking a more serious threat than without.

The company has strict routines in regard of security culture and follows regulations according declarations and reporting. Deviations has not been a problem, and the respondent says he hopes this is because they never happens, not that they are undiscovered. Loyal employees are critical, because there are much information available that can be stolen.

Future use of AMS data

The company has a strong desire to utilize meter data in their power grid management and see the possibilities in using this data with the objective to deliver a better quality of service. Faster response when errors occur and less errors is advantageous for the customers. The company considers the AMS meter as any other sensors in the infrastructure, and hence it is natural to include information from the meters in the power grid planning and management. But it is a necessity to store data for longer periods than as described in the AMS Regulation [27], a limit of 3 years is too short. There is a need to be able to see data from AMS meters in combination with for instance temperature to get good historical analysis. From experiences in the demo project, bottlenecks of capacity exists on different places than expected. This is information that has not been available in the traditional solution. 10 years of historical data might be sufficient but they are unsure in regard of what granularity the data must possess.

Privacy challenges arising from this use of AMS data is the amount of information in these data and the fact that many employees will have access to this information. Loyalty of people working in the company is important. A more critical situation is if the data becomes available to external adversaries. Security becomes more important than before. Awareness of what information lies in this data is important and a it is a challenge to maintain awareness and security in regard of this.

7.2.4 Case study: Tromskraft Nett AS

Status of AMS deployment

Tromskraft Nett AS is currently in the phase of planning and analysis and has not started on defining specifications for the systems yet. There are changes to come in the industry that will take effect in 2020, and to comply with this changes the internal processes in the company are analysed with this in mind. Current solutions for IT architecture are analysed to reveal future requirements. A power supplier centric model where the customers communicates with the electricity distribution companies only will result in big changes in the industry. The goal is to be fully implemented at the beginning of 2018.

When it comes to technical solutions, the idea of the specifications are roughly known, but no details are documented. Reports and documentation from SINTEF will be important during these decisions. The company has a collaboration with other DSOs in regard of acquisitions. According to communication technology, they have not decided anything and there are ongoing cost-benefit analysis. Technical solutions and organisation of the deployment will be outsourced. The installation work will be purchased from another company in the corporation. The company does not posses knowledge and resources to deploy the solution on their own.

Privacy challenges

The company applies to laws and regulations when it comes to security and privacy. AMS data contains more information about each customer, which subsequently results in higher demands of security and privacy. The company has not analysed what practical consequences will come out of this. The switch function has been a topic for discussion. Functionality for mass disconnection is voluntary, but then again this requires a high level of security. There must be well defined routines for the people managing the switch function, but these policies has not been established in the organization yet. The company awaits routines in regard of privacy until the question of where the controller function of meter data will be placed. As long as privacy is handled in a good way, they do not see that privacy challenges will cause any problems. Data must not be leaked, and routines and internal procedures for access to this information must ensure this. Today this is vertically integrated in the company, and everybody has access to data. With AMS there must be a different level of authorization and policies that comply with legislation. Questions regarding technical security is taken care of by the IT department.

The company has not yet any strategy on communication with customers in regard of privacy concerns. They have only informed that the implementation is going to be performed. Some customers has been in contact with the company out of concerns for information about them being at home or not. SCADA is an isolated system, which is a good thing for security but problematic when it comes to communication with other systems. How this will be handled in AMS is subject for discussion. The company have a strong culture regarding security, and there will be a long process before decisions are made. It it obvious that privacy challenges must be handled professionally, and privacy must be communicated more in the company than it currently is.

Privacy by Design is not implemented as a strategy, but the company realise that it is important to take privacy into the planning phase that is going on. They are currently working on documenting where data is stored and transferred. A three-part model with DSOs, electricity distribution companies and a central hub might be advantageous if the controller function is placed with one of these three with a clear division of roles.

Small companies does not have the resources to handle the new challenges arising with AMS, and Tromskraft Nett sees it beneficial to be in a collaboration with other companies when it comes to acquisition and knowledge. Many of the DSOs are not involved in such groups. The smaller the company, the more of such projects as AMS are outsourced. The intermediate sized companies might be in a difficult situation with some internal resources and expertise, but not enough to handle everything on their own.

This is a industry used to technology and systems lasting 50 years and are now converting to information technology where the changes are extremely rapid. There is a gap in knowledge between traditional technology in the power grid and the new in AMS. Traditional systems with proprietary technology are converted to open standard technology where systems must communicate in real-time, and this is challenging according to proper security handling.

Security in information technology is one of the main challenge in regard of privacy, and it is critical to establish policies regarding processing of data connected to the customers. Access control will be important but this will be easier to handle with the three-part model mentioned earlier. It must be stronger security requirements of the routines for processing information. Who shall have access to information about alarms, interruptions, disconnections and payment problems?

Internal routines

The company follows regulations in regard of internal routines, and policies to comply with them will be established. Customers have access to their data of energy usage through an internet application. These portals must include security mechanisms. The smart meters have a standard interface for external devices, and an early idea was that an external display could be connected to this and used to present customer data. Other appliances could also be connected to this interface, for instance washing machines. It makes it easier to use internet as an information carrier and to develop smart solutions for green energy usage. The ambitions in regard of this were high a couple of years ago when the prices of electricity was on the top, but the focus today is more on core functionality where the goal is to move from estimated prices to prices based on time of use and better control of usage.

Contingency, auditing and detection is something the IT function handles. The company has outsourced IT operations and thinks this is beneficial. The security aspect is handled by a third party and from this outsourcing comes a well documented system and a service level agreement. Hence daily operation of the system collecting AMS data might be outsourced, but data will be stored locally and transferred to a central hub. SCADA is not a part of this contract, it is managed internally, and this is positive according to privacy. In addition to the outsourced IT function, the company also have an internal IT group working with some security aspects and security culture.

Future use of AMS data

AMS data must for the company be part of 4 critical systems; Managing meters (verification, control and operation), meter database, grid utilization (incidents, operation, voltage, ground fault), system for work orders to electricians.

Beyond the challenges today, the company does not consider privacy challenges to be more severe in this solutions because the security is principally the same with solid routines and policies. A well documented outsourced IT solution is advantageous according to the respondent.

7.2.5 Case study: Nordlandsnett AS

Status of AMS deployment

Nordlandsnett AS has 30500 end users. The company is part of a cooperation between 7 DSOs, called SMIL, but they have not decided how comprehensive this cooperation will be in the process of acquisition. Nordlansnett has not started the planning phase and awaits the decision to come this autumn about the level of cooperation in SMIL. They have currently about 5000 hourly measured AMS meter installations, and the capacity in the system can reach 18000 end users. Whether or not they will expand this solution is not decided since that will result in a final choice of contractor. Communication technology is PLC between meter and node and mobile communication from node to HES. The plan for investments prepares for a complete deployment of final AMS system in 2016 and 2017.

Privacy challenges

The company has not performed any analysis on privacy challenges yet, and has not worked out any specifications for the system, but privacy concerns is an element that will be considered when this process begins. Access control internally and externally will be of major importance. This will be handled in a good way with the implementation of a central hub for AMS data. The specifications of functionality in that solution will decide what level of security is needed in the company. The last consequence is that either a customer system or meter data system is needed locally. This is an ongoing discussion in the industry.

Secure access of the systems is something the company focus on, for instance enciphered communication channels. The channels today are not enciphered but uses TCP/IP and proprietary ports for communication.

The SMIL group was in the phase of decision of system when the deadline for implementation was postponed from 2017 to 2019. This slowed down the process and the companies are again in the process of continuing the work. It looks like there might be a common specification in the group of DSO, and privacy will be a part of that. They consider it to be beneficial to cooperate on this project to lower the risk.

Access control will be an important element. In a centralized hub such mechanisms will be implemented through that solution and one less task to handle for the DSOs. The industry has a good tradition of securing own systems, but according to privacy there are little experience when it comes to processing personal and sensitive information. It is the amount of data and information that is the biggest challenge. In combination with other data this is a critical challenge in regard of privacy. In a phase of installation it can be a challenge if external contractors are hired in to do some work where they have access to sensitive data. Who is going to visit homes for installation? They are aware of these challenges when hiring third parties to perform tasks on behalf of the company. This will be subject for risk assessments before implementation.

The company is aware of privacy challenges but has not implemented Privacy by Design as a strategy in their AMS project.

The respondent regards security of the communication channels as the most severe challenge when addressing privacy, the respondent emphasize the importance of securing the communication channels. Given that a central hub will be established and be the center of customer services for the electricity distribution companies, the most important task is to ensure secure channels during operational phase and to handle security in regard of personal information during implementation, and security requirements for contractors. This is a critical phase.

The largest DSOs will have to establish automatic processes with policies included during deployment of the AMS system, but the small companies might end up with occasionally ad hoc solutions where privacy and security can easily be neglected. A cooperation with other companies might be positive according this. With a local system for storage of meter data, the link between customer and meter data will be a vulnerable connection.

Internal routines

The company has outsourced their customer service to another company in the same corporation, and security and privacy according to customer information are handled there in compliance with agreements and legislation. Internal systems are subject for access control and only persons that need to access data is granted this access.

Access is not audited, but the access controls are strongly regulated. IT-services are purchased from the corporation and IT security is handled there. The power industry is strictly regulated according to these security aspects. When services are purchased from external parties, for instance customer service, this is regulated by contracts between the companies.

Internal security culture is something the company focuses on. The security culture in the company is prominent, but privacy has traditionally not been a big part of this. They have not taken actions in regard of this yet, but they are aware of the challenges arising. The industry manages a service critical for society, and contingency has been more about functionality over privacy. But an already well incorporated security culture is a positive foundation to build privacy into.

Future use of AMS data

The DSOs are not commercial actors making new services, but they do have interest in the benefit of the investments for a more effective management of the power grid. This depends on how the company can take use of AMS data for delivering a service with better quality to the customers, through analysis, registering interruptions, voltage and output, not just power usage. The goal is a more optimal operation and a better decisional foundation for future investments. The company does not see that this use will compromise privacy in any way more than data from energy usage, but their task is regardless of this to protect the data, since in combination with other sources this can reveal much information about the household activities.

8 Discussion of results

In this chapter the results from the interview project will be subject of discussion. Since the interviews was semi structured and the questions was of an open character, the answers from the respondents was slightly different in regard of scope and level of details. All the respondents hold functions as Project Managers or Project Owners, but one must presume that their core knowledge and background have some differences. The companies are also in different phases in the AMS deployment which also have influenced the answers.

8.1 AMS implementation and technical solutions

8.1.1 Status of implementation

The question regarding the status of the company's AMS implementation was asked to get an overview of where they are in the process of deployment. The argument for doing this is that the answers might reflect their progress and that some of the questions would be difficult to respond to because of that. None of the responding companies have purchased any systems for the final implementation yet. One of them is currently evaluating offers, but the others are working on the specification, analysing system requirements or performing tests prior to the specification. If the deadline for the complete implementation i Norway had not been postponed from 2017 to 2019, the situation might have been different at this point of time, which one of the respondents confirmed in his answer. The process slowed down after the deadline was moved and the companies chose to take a step back and prioritized more time and resources on the planning phase.

All of the respondent answered that they have been awaiting the acquisition phase as long as they feel comfortable with because the development of new technology is fast going, and they want to base their decisions on as much knowledge and experience from demo projects and research reports as possible. There are also ongoing work and discussions in the industry regarding several unanswered questions and unclear situations. The investment in the AMS project for the DSOs is considerable, and they choose this strategy to reduce the risk of not deciding the most optimal solution in regard of functionality and security.

One element all the respondents commented on as a challenging task in the choice of technological solution is the communication technology. Their concern is the challenge in assuring end-to-end security from meter to head end system. A possible outcome is that different technologies will be used between different nodes in the infrastructure, and these technologies handles security in different ways. Such heterogeneous networks might end up having hops of different levels of security. The demo projects was mentioned by several companies as very important areas of research to get knowledge of effective communication technologies and experience from research projects.

8.1.2 Technical solutions

Traditional systems in this industry have been based on proprietary solutions with very long life-cycles in comparison to modern information technology. The companies have gained solid knowledge of these systems over decades and the focus of security has been on functionality and contingency in regard of electricity supply and distribution being a critical system of society. This situation is about to change in AMS where information technology and systems based on open standards are used to perform two-way communication between electricity meters and head end systems (HES). One of the interviewees claimed there is a gap of knowledge in the industry from operating the traditional power grid to AMS and security of communication and IT systems. The purpose of the systems is basically the same, distributing electricity and measuring energy usage, but the information collected in AMS raises privacy and security challenges the industry has not been obliged to deal with earlier.

None of the companies interviewed are going to implement the AMS system only with use of internal resources. External contractors will deliver systems based on specifications made by the company or by assistance of external project management. Some of the companies will purchase the service of installation from another company in the corporation. In some cases they divide the acquisition between technical solutions and business systems and different contractors deliver the solutions respectively. This will result in the need to handle external contractors access to AMS data and other personal information about customers. None of the companies interviewed are going to choose a strategy of outsourcing the whole function of AMS data collection.

The companies faces big challenges in choosing the solutions for their AMS. Knowledge and experience is of vital importance and must exist in the decisional phase, either held by the companies or as outsourced resources.

8.2 Addressing privacy challenges

8.2.1 Legislation, guides and requirements

Three of the companies interviewed said that the legislation they need to comply with and guides presented as tools when preparing the system specifications are unclear and ambiguous when it comes to security and privacy. This makes it more challenging to specify systems that comply with the requirements, and interpretation of what is sufficient security in the AMS system might differ from one DSO to another. A situation where the level of security differ between licensed areas will be very unfortunate. Customers does not have the opportunity to choose which operator to be connected to since this industry is monopolistic and the customers address decides their power grid service provider. There must be an equally sufficient level of security in AMS despite where the customers house is located. It does not exist any certification program for AMS systems in regard of end-to-end security and privacy, and at the time of writing this thesis, there are no arrangement of inspections of how privacy is handled in the systems to ensure an equally sufficiently high level of security with the different grid operators.

Guides and legislation is important foundation and means to ensure that security is properly taken care of in AMS. As the result from the interviews shows, these sources are regarded as unclear and ambiguous which makes it even more challenging to ensure compliance.

According to contracts between DSOs and the customers, the companies are not allowed to measure energy usage based on hourly registrations, only on estimated measurements. At the same time, the Energy Regulation regulates the DSO's right to measure power usage. This is according to the results from the interviews an element of discussion, but before this dilemma is clarified, hourly measurement of energy consumption is illegal. In that respect, the collection of hourly measured energy usage in demo areas and other AMS implementations is illegal as long as a consent is not obtained from the customers with AMS meters installed.

The companies referred to the conflict between the possibilities of obtaining a more efficient operation of the grid by use of AMS data and what is described in the guide from The Norwegian Data Protection Authority [65]. The AMS Regulation's purpose is to contribute to a more effective operation of the power grid in addition to correct measurement of energy usage and invoicing. This is in contrast to the guide that claims "*The Norwegian Data Inspectorate cannot see that there are no other processing purposes other than invoicing which render it necessary to process identifiable personal data*". The AMS-regulation does not mention privacy at all other than a functional requirement of securing data from misuse. According to several of the respondents, this ambiguity is problematic and must in the DSOs opinions be clarified as soon as possible.

The authorities are responsible for preparation of laws and regulations. A situation where interpretation of the legislation can lead to differences in how privacy is handled in the different geographic areas must be avoided. The authorities must strive for a legislation where there are no doubt what the responsibilities for the controllers of the data are, and what is the purpose of data collection. The Norwegian Data Protection Authority's role is to see to that privacy for individuals is attended to and not compromised, and one of their means is to offer guidance based on their expertise. In this situation where the guidelines are seen as indistinct it is necessary to present clearer guides and regulations without contradictions from the authorities to prepare for a standardized sufficient level of security in AMS.

8.2.2 Internal routines

The implementation of AMS will result in some changes in the way DSOs operate and manages the grid, and all the respondents says this is something they work on in their analysing and planning phase prior to final deployment. Legislation and guides are according to the respondents the most important foundation for how they design their organisation of operation. It is important to establish security routines prior and during implementation.

At the same time, none of the companies have implemented Privacy by Design (PbD) as a strategy in their AMS projects, and the respondents are not familiar with the term. This is in contrast with governmental guidelines [45] [67] and risk-assessments of AMS [3]. The concept Pbd is a strategy to ensure that privacy is considered in all stages of a system development, and a mean to reduce the necessity for security and privacy being handled with privacy enhancing technologies (PET) in future projects. The fact that the term PbD is not a part of the AMS project does not necessarily mean that no measures are taken to address the challenges, but it might be an indicator that there is a lack of awareness and clear strategies to handle privacy concerns throughout the project from planning phase to daily operation.

8.2.3 Communication with the customers

None of the companies have established any strategy or started any process of communication with the customers according to the implementation of AMS and privacy concerns. In the two demo projects, the customers involved have received information about the projects, but as one of the respondents says, it is important to broadcast this information at the right time and in the right context. At this point there are too many unanswered questions in regard of privacy, and to start communication at this point might lead to a negative focus in regard of the AMS project.

As mentioned earlier, the two demo projects, Demo Steinkjer and Smart Energy Hvaler have informed their participating customers about the demo activities. When it comes to handling personal information in compliance with the Personal Data Act they have chosen different strategies. In Demo Steinkjer the project has obtained consent from the participating households. In Smart Energy Hvaler the project has defined a demo area and all customers have been included as a part of the project without giving their consent to a defined purpose. The respondent says they anonymize all data before using them in research, but this is not in compliance with the Personal Data Act §8 [10].

According to the AMS regulation, data of energy usage must be available to the customer at 9.00 the next day. The method chosen by the respondents is to make information available to the customers through a web portal. In the specification of the AMS meters, they are to be equipped with a standard interface where an external display can be connected to show energy usage, but this is according to two of the respondent unlikely to be a widespread solution. By the use of a web portal, there must be security mechanisms to ensure that this is not a vulnerable point of attacks from adversaries. Two of the respondents mention that a central hub and a common solution for such portal will be advantageous in the way of targeting the effort of securing one solution instead of 150 portals, one for each DSO. At the same time, a centralized portal will be more valuable to attackers because the amount of data accessible will be considerable larger.

8.3 Knowledge and security culture

The industry of DSOs is strongly regulated due to the fact that they operate a service critical to society. A result of this is a well established security culture in the companies in regard of physical security of the grid, securing the functionality and contingency. With AMS the aspect of privacy becomes increasingly important, and this is a factor the companies has not been obliged to address in the traditional grid. All the respondents mention their strict arrangements of regulations and inspections as a positive aspect, but at the same time they admit that privacy is something they are not used to handle and that there is a need for improvement in this area. The existing security culture is a good foundation to build on, but to implement privacy to be a part of that will include a process of raising awareness and knowledge.

Knowledge and experience was mentioned during the interviews as a critical factor in combination with size of the companies. Small utility companies with little internal resources might choose to outsource or cooperate with other companies in projects or operational tasks involving security and privacy, for instance outsourcing the IT department to take care of IT security, or collaborate with other companies in the process of purchase of AMS systems to ensure that such aspects are handled. Large utility companies often possess knowledge and expertise to manage such tasks in compliance with the requirements, but the risk is the companies that does not fall in any of these two groups. Especially if the perception of the guidelines and requirements in legislation are unclear.

A gap of knowledge is of great importance to address on an early stage of the process. Without knowledge and expertise on information security and privacy the chance of this not being properly addressed from the start of the planning phase is present. It is also important for the companies to be able to perform periodic evaluations of the systems, for which knowledge makes a premise.

Lack of knowledge and awareness is considered a severe threat to information security and privacy, and the consequences might easily lead to unintended threats and privacy problems like insecurity and dissemination as described in chapter 3. An incident resulting in breach of privacy due to unintended or accidental actions is of course negative for the person it affects, but it will also influence the person and the company responsible for the incident. Such incidents will also have a negative effect on the reputation of the AMS project as a whole. During the process of developing the new AMS systems, the companies must ensure that the new operational organization are prepared to handle the new challenges by establishing knowledge and routines in advance to hinder unwanted incidents.

8.4 Future use of AMS data

On the question of future use of AMS data, the respondents feedback are unison. The utility companies wants to use this data to get a positive gain from the AMS investment to operate the power grid in a more effective way. By analysing AMS data in combination with meteorological data they can get valuable information when it comes to future investments and management of the grid, which is also an objective in the AMS Regulation [27]. According to the companies the time period for storing data measured hourly is too short to be of any use (up to 15 months). The argument is that they need to see variations over longer periods of time to have better foundations for analysis. Periods from 3-5 years and up to 10 years storing of hourly measured data are stated as necessary.

The big question in regard of use and protection of AMS data is the definition of the purpose. The respondents are clear on their needs to use this data to gain positive effects from the system, and at the same time the Data Protection Authorities sees the need solely for billing purposes. This ambiguity must be clarified, but the industry should also define on what level of details the data must hold for being suitable for analysis. Solutions where data are anonymized through for instance aggregation points in the infrastructure will enable analysis and at the same time hide information connected to identified persons.

8.5 Future privacy challenges

The most severe privacy challenges can from the interviews be summarized in two categories. First is to secure all the amount of data resulting from AMS and to hinder this data to be exposed and misused by adversaries. Also internal threats like disloyal or careless employees is a critical element. The second category of privacy challenges stated in the interviews are securing the infrastructure, in particular the communication technology and the AMS meters. On the AMS meters, securing them from hacking and manipulation and securing the switch from unintentionally disconnecting the power are important factors.

The challenges in regard of privacy in AMS are numerous, especially since the project involves new responsibilities in a industry used to handle proprietary systems in the traditional power grid. Hence the demo arenas are valuable sources of knowledge and experience and should be used extensively to do research and experiences on how privacy best can be handled to secure the customers personal information of energy usage.

8.6 Summary

The interview project was carried out to find out what privacy challenges the DSOs regard as most severe and how they address the privacy challenges arising from the AMS deployment.

From the companies view, the biggest privacy challenges lies in the amount of information that is available in data collected from AMS meters. And in combination with other sources of information this can reveal detailed information of the activities inside the household. They realize that there is a huge responsibility in managing this data and their focus is on following the requirements in legislation and guidelines from the authorities, which the companies also understand as partly unclear and ambiguous. Another element the companies brought out as vulnerable elements are the AMS meters and in particular the meter switch for restricting and breaking energy outlet. The meters must be secured to avoid hacking, manipulation and to hinder unintended or malignant disconnection. Also the communication technology is a critical element. There are challenges in securing the end-to-end system from meters to head end systems.

The companies also mentioned the fact that the industry, despite of strict regulation and solid security cultures when it comes to securing the power grid functionality, is not used to handle personal data in such amounts and with so abundant information.

To address the challenges of personal information in AMS, the companies focuses on compliance with laws and regulations, but there are according to the results open questions regarding security and privacy that has not been clarified. By following the legislative requirements, routines and mechanisms for deletion, authentication and auditing are analysed and established during implementation of the new operational organization. None of the companies interviewed has introduced PbD as a design principle in their AMS projects, which might be an indicator of a lack of defined strategy of handling privacy through the project.

The demo projects are valuable areas for testing and research for AMS projects as a whole, hence also for security and privacy aspects that needs testing an analysis to find the most secure and functional solution. Gaining knowledge and experiences from these areas are very valuable in the planning phase and during preparation of the system specification.

8.6.1 Validity and reliability

The process of finding respondents to the interview project was somewhat challenging. The starting point was to find respondents which represented companies of different sizes in regard of customers, but the strategy was gradually changed to finding respondents that was positive and able to set down time to participate at all. Whether these companies are representative for the majority of DSOs are therefore questionable. Nevertheless, the impression was that the respondent's answers was very open and honest in regard of what they consider the challenges from their point of view, and what they see as challenges for the whole industry. Since the development in the industry and in technology are continuously ongoing, the results from this interview project is a momentary picture of the situation.

To ensure the quality of the results, the questions was sent to the respondents prior to the interview process. After the interview sessions, the transcript was returned to the respondents to give the opportunity to correct and add information.

9 Conclusion

This chapter gives a summary of the results and findings in this thesis in regard of the research questions.

Privacy challenges in AMS/Smart Grid

To answer RQ1 this thesis has described the complexity of privacy and how privacy problems can arise due to the quality of smart meter data. The challenges are on different levels, both technological and organizational. Advanced Metering Infrastructure (AMI) is vulnerable to a diversity of threats, from the smart meters through communication channels and nodes to the systems of Distribution System Operators (DSO) and a possible data hub. Technological security mechanisms must be implemented to reduce the risk of security breaches, but also organizational means as routines, knowledge and legislation are important in the transition from traditional to a smarter power grid.

How privacy challenges are addressed by DSOs

To answer RQ2 of how privacy challenges is addressed by DSOs, qualitative interviews was performed. The results shows that there are several problems and unanswered questions in regard of security and privacy to be clarified prior to deployment. Legislation and guides are seen as unclear and increases the riskiness in acquisition and deployment. Even though the DSOs operate in an industry with strict regulation an focus on contingency, functionality has been the most important factor up until now, and privacy has not been a concern. The companies must implement information security and privacy as a part of their security culture. The risk is that the gap of knowledge from the proprietary systems to modern information technology and fine-grained meter data results in solutions that does not sufficiently attend to privacy. There is a lack of chosen design strategies like Privacy by Design in the companies AMS projects. Application of PbD in compliance with recommendations from authorities and inspectorate will increase the chance of successful implementation of a privacy preserving system.

The results illuminates the conflict of interests between availability of data for operational use and confidentiality according to privacy principles, and the main challenge is to obtain a solution where both interests are met, both gaining positive operational effects and preserving the customers privacy.

Data from smart meters

In order to answer RQ3, literature study and a data analysis was performed to illustrate how data from smart meters can be used to describe habits and activities inside a customers home. Requirements of functionality as described in the AMS Regulation [27] is that electricity usage are to be measured every 60 minutes with the possibility to change the frequency to every 15 minutes. A data analysis of smart meter data from one of the demo areas shows that information about household activities are revealed. If in the future the measuring frequency is calibrated to shorter intervals, even more detailed information becomes available.

Future use of AMS data

It is hard to foresee the development of products and services in the wake of full AMS implementation. DSOs are not commercial actors in the market of such services, but has an interest in using this data in planning and operation of the power grid. Non-Utility Service Providers (NUSP) offers new products to energy customers by means of their energy usage data. In order to answer RQ4 this thesis has suggested different means to the challenge of ensuring that privacy is not compromised as a result of new application of smart meter data. Awareness and knowledge of information security becomes increasingly important with all stakeholders, and a defined and unambiguous legislation together with an arrangement of inspections is necessary as a foundation to obtain a sufficient and equally secure handling of personal information for all inhabitants.

10 Future work

This chapter presents some suggestions for further research on this thesis topic.

Selection of respondents

As mentioned in the section discussing validity and reliability, respondents to the interview projects was limited to companies with positive response on the request of participation. To ensure a more valid result, it might have been a more optimal situation to chose respondents in different sizes according to customers and another geographical diffusion. Since collaborations between DSOs often is based on their adjacent areas of operation, several of the respondents in this thesis interviews represented the same collaboration in which might be unfortunate in regard of generalising the result to the industry as a whole.

Since the interviews had a qualitative approach, the need for several respondents for statistical analysis was not a goal. Nevertheless, it might have been interesting to map out how a larger number of DSOs addresses privacy challenges by performing a questionnaire with questions of a more concrete character.

Case studies later in AMS deployment

A situation that changed the angle of this thesis during the period of writing was when the deadline for complete implementation was postponed from the beginning of 2017 to 2019. This decision resulted in a slowing down of the process of planning and acquisition of technical solutions in the AMS projects. According to the respondents, this was a favourable decision because there was a need for more time to do planning, analysing and to consider different technologies. According to the report of AMS status from February 2012 (before the deadline was postponed), most of the DSOs planed implementation during 2015 and 2016. The interview results indicates that implementation in 2017 and 2018 is a more accurate estimation after the new deadline.

At a later point of time in the implementation process, there would have been possible to do the same case studies in combination with technical analysis to assess how technical security have been implemented in accordance to privacy concerns. Another aspect available for analysis on a later point of time is internal routines in the organization of operation since most of the respondents stated that the determination of new routines is an ongoing process.

Legislation and regulations have been characterized as unclear and ambiguous by the respondents, and there is an ongoing discussion in the industry on this challenge. If privacy and/or energy related legislation is changed or expanded during the time until final implementation, the premisses for doing such case studies is changed and a would probably give another conclusion.

From customers point of view

Most of the DSOs has not prepared any strategy of communication with the customers [68], which was confirmed in the results from the interviews. Even though the customers normally cannot option out the installation of a smart meter, the acceptance by the customers are important for the AMS project and in future development. After implementation is completed, it would have been an interesting case to examine how the implementation has affected the customers, their knowledge and awareness of privacy concerns in AMS.

Non-Utility Service Providers

How the marked of third-party service providers will develop after final implementation of AMS in Norway is difficult to foresee. Some products and services exists already and it is presumable that this marked will increase after the deadline in Norway in 2019, and EU in 2022. A future study might look into how personal information are handled in NUSP services and how privacy concerns are taken care of.

Bibliography

[1] Siddiqui, F., Zeadally, S., Alcaraz, C., & Galvao, S. 30 2012-aug. 2 2012. Smart grid privacy: Issues and solutions. In *Computer Communications and Networks (ICCCN), 2012 21st International Conference on*, 1 –5.

[2] Sand, K., Nordgård, D., Benum, T., Foosnœs, J., Kristoffersen, V., & Wåge, D. June 2013. Experiences from norwegian smart grid pilot projekts. *CIRED*.

[3] Tøndel, I., Jaatun, M., & Line. 2010. Security threats in demo steinkjer. *SINTEF*.

[4] Solove, D. 2006. A taxonomy of privacy. *University of Pennsylvania Law Review*.

[5] Fang, X., Misra, S., Xue, G., & Yang, D. 2012. Smart grid - the new and improved power grid: A survey. *Communications Surveys Tutorials, IEEE*, 14(4), 944–980.

[6] Leedy, P. & Ormrod, J. 2005. *Practical Research - Planning and design*. Pearson Merrill Prentice Hall.

[7] Lu, Z., Lu, X., Wang, W., & Wang, C. 31 2010-nov. 3 2010. Review and evaluation of security threats on the communication networks in the smart grid. In *MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010*, 1830 –1835.

[8] Efthymiou, C. & Kalogridis, G. oct. 2010. Smart grid privacy via anonymization of smart metering data. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 238 –243.

[9] Quinn, E. L. 2008. Privacy and the new energy infrastructure. *Center for Energy and Environmental Security*.

[10] Lovdata. Lov om behandling av personopplysninger (personopplysningsloven) / Personal Data Act 2000-04.
`http://www.lovdata.no/all/hl-20000414-031.html`, September 2013.

[11] Williams, M.-A. aug. 2009. Privacy management, the law and business strategies: A case for privacy driven design. In *Computational Science and Engineering, 2009. CSE '09. International Conference on*, volume 3, 60 –67.

[12] Sankar, L., Kar, S., Tandon, R., & Poor, H. oct. 2011. Competitive privacy in the smart grid: An information-theoretic approach. In *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, 220 –225.

[13] AlAbdulkarim, L. & Lukszo, Z. april 2011. Impact of privacy concerns on consumers' acceptance of smart metering in the netherlands. In *Networking, Sensing and Control (ICNSC), 2011 IEEE International Conference on*, 287 –292.

[14] Gharavi, H. & Ghafurian, R. 2011. Smart grid: The electric energy system of the future [scanning the issue]. *Proceedings of the IEEE*, 99(6), 917–921.

[15] Karnouskos, S. The cooperative internet of things enabled smart grid.

[16] McDaniel, P. & McLaughlin, S. may-june 2009. Security and privacy challenges in the smart grid. *Security Privacy, IEEE*, 7(3), 75 –77.

[17] NTE. Demo steinkjer.
`https://www.demosteinkjer.no/`.

[18] Fredrikstad Energi AS. Smart energi hvaler.
`http://www.smartenergihvaler.no/`.

[19] Statnett. Statnett skal utvikle datahub for kraftmarkedet.
`http://www.statnett.no`, September 2013.

[20] Statnett. Dansk-norsk intensjonsavtale om datahub.
`http://www.statnett.no`, September 2013.

[21] Line, M., Johansen, G., & Saele, H. 2012. Risikovurdering av ams. *SINTEF*.

[22] NVE. Concessions for geograhic areas.
`http://www.nve.no/no/Konsesjoner/Nett/Omradekonsesjoner/`, September 2013.

[23] Wokutch, A. The role of non-utility service providers in smart grid development: should they be regulated, and if so, who can regulate them?
`http://www.jthtl.org`, November 2013.

[24] Coetzee, L. & Eksteen, J. 2011. The internet of things - promise for the future? an introduction. In *IST-Africa Conference Proceedings, 2011*, 1–9.

[25] Ou, Q., Zhen, Y., Li, X., Zhang, Y., & Zeng, L. 2012. Application of internet of things in smart grid power transmission. In *Mobile, Ubiquitous, and Intelligent Computing (MUSIC), 2012 Third FTRA International Conference on*, 96–100.

[26] Covington, M. & Carskadden, R. 2013. Threat implications of the internet of things. In *Cyber Conflict (CyCon), 2013 5th International Conference on*, 1–12.

[27] Lovdata. Forskrift om endring i forskrift om måling, avregning og samordnet opptreden ved kraftomsetning og fakturering av nettjenester (energilovforskriften) / Energy Regulation 1990-06-29.
`http://www.lovdata.no`, September 2013.

[28] Marmol, F., Sorge, C., Ugus, O., & Perez, G. May. Do not snoop my habits: preserving privacy in the smart grid. *Communications Magazine, IEEE*, 50(5), 166–172.

[29] Datatilsynet/The Norwegian Data Protection Authority. Personvern.
`http://www.datatilsynet.no/personvern/Hva-er-personvern/`, September 2013.

[30] United Nations. The Universal Declaration of Human Rights. `http://www.un.org/en/documents/udhr/index.shtml`, September 2013.

[31] Eco, U. 2008. *Turning back the clock*. Vintage books.

[32] Apenes, G. 2005. *Fra tillitt til kontroll - Tolv samtaler om politikk, teknologi og personvern*. Pax Forlag.

[33] Stanford Enclyclopedia of Philosophy. Privacy. `http://plato.stanford.edu/entries/privacy/`, September 2013.

[34] Warren, S. D. & Brandeis, L. D. The right to privacy. `http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm`, September 2013.

[35] Fornyings-, administrasjons- og kirkedepartementet. Hva er Personvern? `http://www.regjeringen.no`, September 2013.

[36] Konupek, M., Bing, J., Omdahl, S. E., Luders, M., Greve, V., & Svendsen, L. F. 2010. *Til forsvar for personvernet*. Universitetsforlager.

[37] Orwell, G. 1949. *Nineteen Eighty-Four*. Secker ans Warburg.

[38] Charlie Chaplin, United Artists. Modern Times. `http://en.wikipedia.org/wiki/Modern_Times_(film)`, 1936.

[39] Ibsen, H. 1890. *Hedda Gabler*. Henrik Ibsen.

[40] European Union. Directive 2006/24/EC. `http://europa.eu/eu-law/legislation/index_en.htm`, September 2013.

[41] Wikipedia. PRISM (surveillance program). `http://en.wikipedia.org/wiki/PRISM_(surveillance_program)`, September 2013.

[42] Jansen, A. and Schartum, D. W. (red). 2005. *Informasjonssikkerhet - Rettslige krav til sikker bruk av IKT*. Fagbokforlaget.

[43] Gollmann, D. 2006. *Computer security*. Wiley.

[44] Norges offentlige utredninger 2013:2. Hindre for digital verdiskaping. `http://www.regjeringen.no`.

[45] Administrtasjons- og kiredepartementet. Meld. St. 11 2012-2013 Personvern - utsikter og utfordringar. `http://www.regjeringen.no`.

[46] Loewenstein, G., John, L. K., & Acquisti, A. 2009. The best of strangers: Context dependent willingness to divulge personal information. In *Social Science Research Network*.

[47] Datatilsynet/The Norwegian Data Protection Authority. Personvernrapporten 2010. `http://www.datatilsynet.no`, September 2013.

[48] European Union. Directive 95/46/EC.
`http://europa.eu/eu-law/legislation/index_en.htm`, Oktober 2013.

[49] Lovdata. Forskrift om behandling av personopplysninger (personopplysningsforskriften) / Personal Data Regulation 2000-12.
`http://www.lovdata.no/for/sf/fa/xa-20001215-1265.html`, September 2013.

[50] Lovdata. Lov om produksjon, omforming, overføringringring, omsetning, fordeling og bruk av energi m.m (energiloven) / Energy Act 1990-06-29.
`http://www.lovdata.no/all/hl-19900629-050.html`, September 2013.

[51] OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
`http://www.oecd.org`, September 2013.

[52] Eurpean Council. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
`http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm`, September 2013.

[53] Liu, T., Liu, Y., Mao, Y., Sun, Y., Guan, X., Gong, W., & Xiao, S. 2013. A dynamic secret-based encryption scheme for smart grid wireless communication. In *IEEE*.

[54] Liu, Y., Ning, P., & Reiter, M. K. June 2011. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.*, 14(1), 13:1–13:33.

[55] Ayday, E. & Rajagopal, S. 2011. Secure, intuitive and low-cost device authentication for smart grid networks. In *Consumer Communications and Networking Conference (CCNC), 2011 IEEE*, 1161–1165.

[56] Vigo, R., Yuksel, E., & Ramli, C. 2012. Smart grid security a smart meter-centric perspective. In *Telecommunications Forum (TELFOR), 2012 20th*, 127–130.

[57] Line, M. 2013. A case study: Preparing for the smart grids - identifying current practice for information security incident management in the power industry. In *IT Security Incident Management and IT Forensics (IMF), 2013 Seventh International Conference on*, 26–32.

[58] Rache, G. 2012. Intrusion detection system for advanced metering infrastructure. In *EPRI*.

[59] Hart, G. dec 1992. Nonintrusive appliance load monitoring. *Proceedings of the IEEE*, 80(12), 1870 –1891.

[60] International Working Group on Data Protection in Telecommunications. 2011. Privacy by design and smart metering: Minimize the personal information to maintain privacy. In *Working paper*.

[61] Cavoukian, A. & Kursawe, K. 2012. Implementing privacy by design: The smart meter case. In *Smart Grid Engineering (SGE), 2012 IEEE International Conference on*, 1–8.

[62] Privacybydesign.ca. Privacy by Design:Achieving the Gold Standard in Data Protection for the Smart Grid.
http://www.ipc.on.ca/images/Resources/achieve-goldstnd.pdf, September 2013.

[63] Boritz, E. & No, W. G. Aug. A gap in perceived importance of privacy policies between individuals and companies. In *Privacy, Security, Trust and the Management of e-Business, 2009. CONGRESS '09. World Congress on*, 181–192.

[64] Kvaale, S. & Brinkmann, S. 2009. *Det kvalitative forskningsintervju*. Gyldendal akademisk.

[65] Datatilsynet/The Norwegian Data Protection Authority. Guide for processing of personal data in connection with automatic metering systems within the energy sector.
http://www.datatilsynet.no, October 2013.

[66] Lovdata. Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften) / Contingency Regulation 2012-12-07.
http://www.lovdata.no, September 2013.

[67] Datatilsynet/The Norwegian Data Protection Authority. Innebygd Personvern.
http://www.datatilsynet.no/Teknologi/Innebygd-personvern/, September 2013.

[68] NVE. Notat - rapportering om status og planer for ams.
https://www.nve.no/.

A Appendix

A.1 Questions for semi structured interview

Background

1. What is the status of the AMS deployment in the distribution area of the company?
2. What is the technical solution chosen for the AMS (if chosen)?

Privacy

1. How do the company organize the work to address security and privacy challenges?
2. How does the company communicate privacy concerns to their customers?
3. Does the company take use of design principles of privacy-by-design?
4. What privacy challenges does the company consider as the most severe in AMS?

Internal routines

1. Does the company have routines established to delete or hand out data on customers request, or deleting after the purpose is outdated?
2. Is the company prepared to handle incidents according to security and privacy in AMS?
3. Does the company take initiatives in regards of internal security culture?

Future applications

1. Plans or thoughts about future application of data from smart meters?
2. Thoughts about privacy challenges arising from future application of smart meter data?