Architecture of the Smart Grid affects privacy

Jussi Laakkonen, Salla Annala, and Pekka Jäppinen,

***Abstract*—From the electricity companies point of view the customer is traditionally seen only as a consumer but with new technology and more intelligent electricity network things are about to change. As the customer activity is attempted to be increased with the help of Smart Grid environment new concerns about the privacy of the customers rise. This paper covers the risks and threats related to different connections between various actors in Smart Grid environment including the risks and threats against the information systems of different actors. The environment is presented as a reference architecture which is based on existing implementations and the results of a questionnaire. For creating the reference architecture an abstract architecture was derived and is presented in this paper. The abstract architecture contains the different tasks that are required in such environment including the data flow between the tasks. The reference architecture is used to analyze the risks and threats with customer privacy in mind. As an result the threats are identified and an initial solution for protecting customer privacy is presented.**

***Index Terms*—privacy, smart meter, smart grid, risk assessment, threat analysis**

I. Introduction

THE energy markets are moving towards more efficient electricity distribution systems and also the energy consumption-awareness of consumers is intended to be increased in the future with the help of smart meters collecting and sharing electricity consumption data. For the electricity networks the smart meters will provide a valuable tool that can be used to balance the load of the network. The more detailed the consumption information and the control capabilities the smart meters can provide opens up questions how it all affects to customer privacy. New issues arise as researchers investigate different aspects of the area, for example it has been recently discovered that TV watching habits[1] or even the watched content [1] can be extrapolated from the consumption data.

These threats have not been gone unnoticed and, in addition to EU directives and country laws for record keeping and personal information handling, new directives have been made specially for the energy markets. In the directives 2006/32/EC[2] and 2009/72/EC [2] it was recommended that, if assessed financially reasonable, consumers must be equipped with intelligent metering systems that provide information on customer's actual energy consumption and time of use. In [2] the deadline for equipping at least 80 per cent of consumers with intelligent, or in other words, smart meters was set to 2020. The directives (aimed more towards electricity markets) and laws define the basic level for protecting the privacy of the customers. As the field in implementations of smart metering systems is fairly wide (e.g. in Finland) the directives and laws cannot keep up with the risks or cover all possible threats. The electricity consumption data poses the biggest risks towards customer privacy; it is yet undecided that what the data contains, who stores the data and who can access the data. Let alone the threats the various, potentially unsafe, data transmission methods bring.

In the future electricity systems the actions of the customers have a major impact on the electricity system as the customers control the long and short term energy consumption and, therefore, the interactive customer is seen as active resource in the system. For this to become reality, it is imperative to ensure that the customers would accept and trust the new Smart Grid environment collecting their private measurement data on hourly basis. Previous studies show that one of the biggest issues in establishing customer trust in this case is that the privacy is built into the design and the customers can see that their privacy needs are taken care of.

The aim of this paper is to identify the risks and threats in Smart Grid environment so proper guidelines for protecting the privacy of the customers can be provided. As previous studies show different players even within Finland not to mention in Europe or world, tend to share the tasks differently between accompanying companies. For this reason we have created an abstract reference architecture, which is used for privacy analysis. Also an analysis of the effects of different data sharing schemes used by the different actors is provided.

In the following sections, based on the defined architecture, the risks and threats on the communication pathways are analyzed and the possible results of each threat coming true are assessed. The paper is structured as follows; second section covers the related work on privacy in Smart Grid environment. The third section presents the questionnaire results and analysis along the reference architecture including its actors and connections. In the fourth section the threats and risks related to the information systems of the actors and the connections between them are evaluated. In the fifth section the changing roles and the effect on privacy is analyzed. The sixth section introduces a mitigation plan for enhancing the customer privacy based on the reference architecture along the future work description. The seventh section concludes the paper.

II. Related Work

As the smart metering systems have not been long in the market some pilots have emerged to field test the systems as a whole and as the results of these pilots new concerns about customer privacy have arisen. Some research has been done about the customer privacy in the upcoming and piloted systems.

[1] http://events.ccc.de/congress/2011/Fahrplan/events/4754.en.html

[2] European Parliament and Council, "Directive 2006/32/EC on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC"

Anderson and Fuloria have analyzed the privacy in smart metering systems as a whole keeping the UK situation in mind [3], in which they have made some recommendations for smart meters. In [3] one of the main points was to warn that the electricity metering project of the UK government might not succeed because of customer mistrust, divergence of electricity generators resulting in complex control of the meters and the possibility of conflicts with the measurement data distribution and ownership. As an conclusion they stated that an independent energy regulatory authority (ERA) should manage the metering network and the customer should own the data, which is forced to be shared with the utility to limited extent. In addition to these it was recommended that the distribution of data should be guaranteed by standardized methods between different actors. They recommend that demand management and the auditing of data should be left for the distribution system operators (DSO). The architecture used in the UK differs from one that is commonly used, in EU member states the DSO is responsible of the metering but in UK it is more common that the retailer handles also the distribution and, therefore, handles also the metering. Here we present a scenario where these two can be two different companies. This brings new challenges for customer privacy as the information is even more distributed among different participants. In this paper we are using the recommendations as guidelines for our own analysis about the threats in Smart Grid environment and inspect the different actors, including the connections between them, in the environment more closely.

The second paper of Anderson and Fuloria [4] is concentrating more on the threats of malicious usage of the smart meters. They propose a scheme for managing the certificates in the smart metering application architecture. Their proposed scheme, or an architecture as they state in the paper, takes account of the shared control of devices, changing of electricity retailer, software upgrades and cyber attacks. It is also suggested that the created standard for managing the smart meters and its testing plan should be, as they state in the paper; “subjected to open peer review”. The proposition about the usage of Public Key Infrastructure (PKI) for shared control of the devices is adopted into our design to ensure secured and verified data transmissions between the smart meters and the reader of the meters. The granting of access into the meters can be done as proposed; the manufacturer authorizes certain parties to access the meters directly.

The effectivity of data mining techniques with electricity consumption data has been demonstrated in the research of Lisovich and Wicker [5]. Their research shows that the metering data gives quite accurate information about the resident and his/her behavior which can be then exploited by, e.g. criminals or other interested parties. The data for the research was gathered from a two week long small scale smart metering experiment conducted in the USA. From the gathered data the presence and the sleep cycles of the resident were estimated with high confidence. The results of the research suggests that the resolution of the metering information should be decreased when information is shared among other participants to make the data mining techniques less effective. They also suggest that extensive averaging of the events could be used for masking the events which have fairly short intervals between ’on’ and ’off’ events. Based on this information about the consumption data we adopt the low grained information sharing for third parties who analyze the consumption data. For parties who actually require more detailed information (DSO, electricity retailer, and ERA) the resolution of the information cannot be reduced as it would not fulfill the requirements.

As the papers [3], [4], [5] present valuable insight about the customer privacy in certain areas of the Smart Grid environment they are not, however, considering the environment as a whole. Our aim is to provide an overall view into customer privacy threats in the whole Smart Grid environment.

III. The architecture for Smart Grid environment

To properly analyze the potential risks towards privacy, it is important to know the various functionalities and conducted communication in Smart Grid environment. Since the pilot projects and existing implementations tend to vary we have created an abstract and a reference architecture for analysis. The abstract architecture has been created by analyzing the published results of aforementioned implementations [6], [7] to gather the required functionalities in the environment. Additional information was gathered by conducting a questionnaire that was sent to all DSOs in Finland. The connections between different actors in the reference architecture were derived from the results and most common ones were selected. The reference architecture allows evaluation of the most common threats on different connections between different functionalities in the environment. The abstract architecture enables the evaluation of the risks and threats without concentrating on who is taking responsibility of the tasks. Following section goes through the risks and threats related to different connection pathways and actors in the presented architecture.

A. Architecture analysis

The previous pilots [6], [7] provided information about the current implementations, this information is used for first identifying the tasks for abstract architecture and then creating the reference architecture by assigning tasks to different participants in the environment. Also a questionnaire was conducted to to gather information about the approaches used in current smart metering systems in Finland and also to gather the readiness of DSOs when moving towards smart metering systems. The questionnaire was devised by Laboratory of Electricity Markets and Power Systems of Lappeenranta University of Technology and was conducted between August and September 2011. Total of 30 DSOs answered to the questionnaire. As total these DSOs cover 49 per cent of all electricity customers in Finland.

The results the pilots provided varied a bit but in general the implementations did contain similarities. In both pilots the reading and controlling tasks were assigned to a telecommunications operator, which also provided the infrastructure for accessing the smart meters. The communication between the smart meters and the telecommunications operator was done over mobile phone networks and, in some cases, serial port connections or mesh networks were utilized when possible.

The ownership of the measurement data information system (MDIS), however, varied; in [6] it was owned by the telecommunications operator but in [7] the DSO had the full ownership of the information systems. The smart meters collected hourly readings on the electricity consumption and the data was read from the meters once a day in both pilots. Both DSOs did provide a web interface for their customers for monitoring own electricity consumption and also for authorizing a trusted third party (TTP) to have access to the data.

The results of the questionnaire show that the system used for reading the data from meters is usually owned by the telecommunications operator but the meters are owned and maintained by the DSOs. In every case the telecommunications operator is involved it reads the measurement data from the smart meters and does the updates (software and tariff updates) to the meters as well. The most common technique for communicating with the smart meters is using wireless techniques, usually 2G or 2.5G/GPRS (General Packet Radio Service)mobile phone network. However, half of the DSOs use the electric grid to transfer the measurement data and there are still a few who use traditional copper-wired telephone network. Only a few send the data over public network while most of the DSOs use a private network; either a private mobile phone network or a Virtual Private Network (VPN), which is usually provided by the telecommunications operator. Only in 60 per cent of the cases the measurement data is transferred using a standardized method, while rest are using a proprietary method.

In the slight majority of the cases the maintenance of the measurement database belongs to the DSO and only in every fourth case the telecommunications operator has a copy of the database. In half of the cases the telecommunications operator can write to and read from the database. In most of these cases the DSOs can also manage the database contents.

Currently the most common way to identify the source of the measurement data is to use the serial number of the meter. In 17,5 per cent of the cases the identification is done with IP (Internet Protocol) address and in 10 per cent of the cases an combination of IP address and the meter id is used. Only in 7,5 per cent of the cases the location of the meter, possibly the address of the residence, is used as identification.

Only in every third case the time that the data is kept in the meters was more than six months, the most common time period being from one to six months. Only in 10 per cent of the cases the data was kept for less than one month in the meter. Depending on the meter type they are capable of logging real power, reactive power, electric current, phase voltage, interrupts, errors in grounding and/or voltage levels in addition to the hourly electricity consumption. The electricity consumption was usually read once per day which is set as minimum level by Finnish Council of State decree 66/2009 [8]. Voltages, real and reactive powers were usually read from the meters when needed. The reading of the interrupts varied the most, the most common ones being when needed (56 per cent) and daily (26 per cent).

Based on the results of the pilots and the questionnaire there is no common architecture model and the solutions used by different DSOs vary a lot. The model, its actors and connection techniques have a major effect on customer privacy analysis as the differences might pose new threats, or in some cases, reduce the risk. To fully evaluate the concerns about privacy a common model needs to be selected. Here we address the issue with an architecture that follows the most general approach that was extracted from the questionnaire results influenced with the architecture used in the pilots [6], [7].

B. The abstract architecture

The abstract architecture is a generalized model derived from the more detailed model used in Smart Grid environments, which is usable in other similar deployments for analyzing the privacy threats. It is designed to be used as a tool in threat analysis process for identifying the tasks of actors and then creating the reference architecture. The abstract architecture contains the different tasks and access levels to the information and takes no other stance on the connections between participants than the task requires. For example, the accesser and the processer of the information must be connected to the information storer/keeper in order to access or process the information.

In a architecture similar to the Smart Grid environment the common parts are information source, reader, controller storer/keeper, accesser and processer as presented in Figure 1. Each of these have different access levels to the provided information based on their tasks. The quantity of the participants is irrelevant in this architecture, however, there usually is one reader reading from multiple sources, who provides the data to one or multiple storers/keepers. The accesser task can be executed by multiple different participants and they are either getting the information from storers/keepers or also saving it and, therefore, acting as storers/keepers themselves too. The information prosesser task requires access to the data and the level depends on the role of the processer. The arrow in Figure 1 represents the information flow between the tasks.

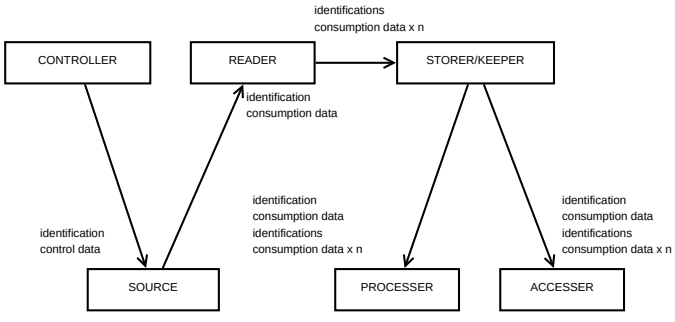

Figure 1. Tasks and data flow in the abstract architecture

The information source naturally has full access to the information as it provides the information for the reader. The reader can access all the data the source provides and also can control the devices at the source site, however, this can be a separate task too if the architectural design requires it. The storer/keeper gets all information from the reader only and naturally stores the information into a database. As mentioned, there can be multiple different participants accessing this information, these participants can, and usually

have, different level of access to the information. The access level is defined by the task the participant is executing, e.g., in real world situation; Smart Grid environment, the electricity retailer should get more detailed information than the third party analysis service gets. It is also possible that the tasks are combined within one participant. The third party could, for instance, access the source site devices directly to get information for analysis. Same applies also for the participants processing the information as they require some access to the information in order to process the data.

C. The reference architecture

The effect of the results of the pilots and the questionnaire to the architecture are limited to the use of the communication techniques and the varying responsibilities in management and ownership of the different information systems. The sizes of the logs or the information they contain have no effect on the architecture itself. The division of the responsibility of the database management is quite diverged as the results show. Based on this information the reader (usually a telecommunications operator) in the presented reference architecture has a separate MDIS which covers the whole measurement system, including reading from the meters. The DSO has own, separate information system for customer data; customer data information system (CDIS).

The overall architecture consists of different actors, networks and connections over these networks as shown in Figure 2 with threat levels assigned to connections. These threats are analysed and explained in the fourth section of this paper. Table I covers the different actors and their roles in the architecture. Actors are identified with an actor identifier (AID). The essential parts in all of the smart grid implementations are the smart meter, smart meter reader and billing information system, and, in addition, there are different databases containing customer information. From the existing implementations we found out that communication between meter and the reader is done over mobile networks [6], [7]. For the deployment of different databases and connections between the actors the questionnaire provided some additional information. In addition to this the questionnaire gave insight about the data stored in the meters. In table II the mapping between different tasks in the abstract architecture and the actors in the reference architecture are presented. The connection pathways in Figure 2 are explained in Table III, each connection having an unique connection identifier (CID).

The data to be sent is assumed to contain personal identifiable information (PII) and the electricity consumption data. As in the previous pilots [6], [7] it is also assumed here that the electricity consumption is measured hourly and sent once per day from the meters to the MDIS (over CID 3 in Figure 2). In this architecture the maintenance and the updates are assumed to happen via the reader (using CID 3) and the DSO only requests the consumption data from the MDIS (via CID 4 in Figure 2). The electricity retailer does not have direct access to meters as it needs only the total amount of consumed electricity, this is provided by the CDIS of the DSO (via CID 6 in Figure 2).

Table I
ROLES OF DIFFERENT ACTORS

AID	Actor name	Role
I	Customer	The customer who owns of the residence. Makes contract with the DSO for delivering electricity and also decides whether to share consumption information with a TTP.
I.a	Smart Meter	Smart meter keeping track of electricity consumption and other related activities. Contains local log information about the electricity consumption of the residence.
I.b	Meters	Various meters used in the residence e.g. thermostats, water meters, etc. Provides information for Smart Meter about appliances and their energy consumption.
I.c	Sensors	Various sensors in the residence e.g. temperature sensors. Provides information for the selected meters.
I.d	Resident	The end-user in the residence who is not necessarily the owner of the residence. Monitors own electricity consumption via web-based interfaces provided by the DSO and/or TTPs.
II	Reader	Smart meter reader responsible of the communications between the Smart Meter and the MDIS.
II.a	MDIS	Information system and database containing all measured consumption information of every customer using Smart Meters. Provides consumption information for CDIS (III.a) when requested.
III	DSO	Provides electricity distribution to customers via electricity grid. Maintains CDIS (III.a).
III.a	CDIS	User database and information system. Contains details about customers, billing information, consumption information, etc. Requests consumption information from MDIS (II.a).
III.b	Client personal user interface	Interface for customers to view billing information, contract details, general consumption details and to see and change own information. Information is provided by CDIS (III.a).
IV	Electricity Retailer	Electricity provider. Charges customers based on the readings provided by DSO (III).
IV.a	Billing information system	Information system for customer billing. Contains the total electricity consumption data of each customer.
V	ERA	Official independent energy market regulator.
VI	TTP	Trusted Third Party providing long term analysis of the consumption data which is provided by DSO and agreed by the customer.
VI.a	TTP information system	Information system and database of the TTP containing raw and analyzed data of the customers who have made a deal with the TTP. Information is provided to authenticated customers via WWW interface (VI.b).
VI.b	TTP client user interface	Interface for customers to see the analyzed consumption data.

IV. RISKS AND THREATS

This section presents the risks with each communication pathway and introduces possible threats on each, including analysis of the threats of the information systems insecurity brings towards the customer privacy. The threats we are dealing here are related to common threats for wireless mediums and to open Internet; information is lost during transmission, information is manipulated or corrupted on the pathway, information is captured during transmission or the database security is breached.

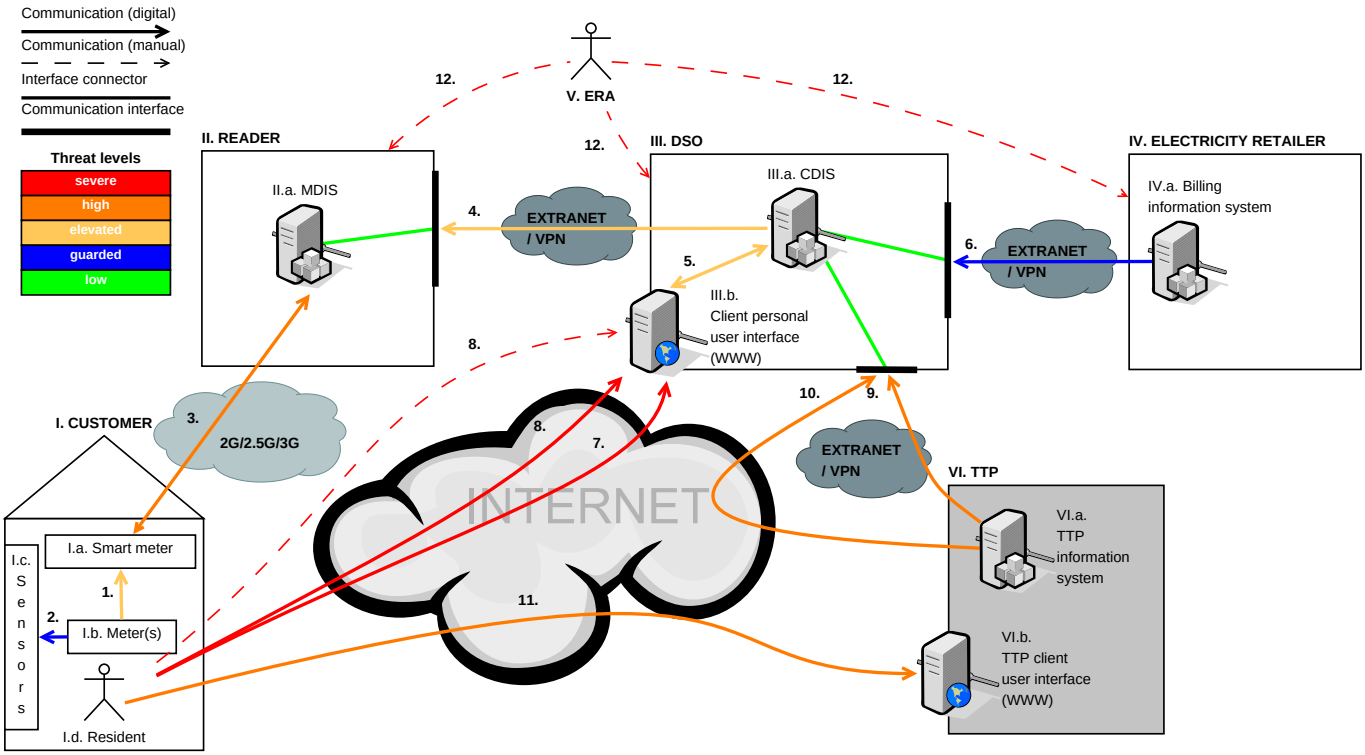

Figure 2. The reference architecture

Table II
MAPPING OF TASKS TO ACTORS

Task	Role	Actor	Access to data
Source	Provide metering data	I	Full
Reader	Read metering data	II	None, pass through
Controller	Control the meter	II	Low
Storer/keeper	Store the metering data	III,IV,VI	Full
Accesser	Access the metering data	I,III,IV,V,VI	Dependant on the actions
Processer	Process the metering data	III,IV,VI	Dependant on the actions

A. Lack of standards

The lack of standardized and open methods is not addressed in the architecture but in order to build customer trust this issue should be taken into account. It is better to openly tell to the customers what is read from their meters and how than to hide it and try to convince that nothing more, than the contract states, is read. This calls for cooperation between the ERAs and the industry to build a common rules, preferably an open interoperability standard for reading data from the smart meters and ensuring proper precautions when storing the data. This would have an increasing effect on customer privacy and it would also make the auditing of the companies much more effective, as also stated by Anderson and Fuloria in [3].

B. Consumption data storage

The architecture does not take any stance on the data storage issue on meters or on information systems. According to EU directive 2009/72/EC article 40 [2] the relevant data related to all transactions should be kept for five years. In Finland the consumption data is required to be kept for six years by Finnish Council of State decree 66/2009 [8]. Although the DSOs and the retailers might not necessarily need the long term consumption data for billing purposes and the amount of data collected from the five or six year period poses a privacy threat in case of database breach, it is necessary to follow the regulations. It would help the companies in their internal audits as it was recommended by Anderson and Fuloria [3] that the companies carry the “heavy lifting” in the auditing process.

The amount of the consumption data in the databases brings new challenges for storaging. The data one DSO has of its customers might not be possible to put into one single database hence the vast amount of data. It has been estimated that by 2020 there are over 238 million smart meters deployed in Europe[3]. As total these meters would generate 5217 million consumption data entries per day whereas a DSO with 100 thousand customers would get 2,4 million consumption data measurements in one day. In [3] it was mentioned that in USA with rate of four measurements per hour about half a million smart meters generate 200 TB of data in one year, resulting in an estimate of 107 MB worth of measurement data per meter in year if consumption is measured once per hour. The space requirement of one consumption data entry is roughly 12 kB, which would result in c.a. 28 GB of data in one day with 100 thousand customers. Therefore, distributed physical databases or cloud computing solutions would be

[3]http://www.pikeresearch.com/newsroom/238-million-smart-meters-to-be-deployed-in-europe-by-2020

Table III
CONNECTION DESCRIPTIONS

CID	Network	Description
1.	Home Area Network (HAN)	Read data from various household meters and/or sensors.
2.	HAN / Wireless	Read data from sensors in the household.
3.	2G / 2.5G / 3G / Electric Grid	Sending and/or requesting measurement data from smart meter or sending tariffs to smart meter.
4.	Extranet / VPN	Information exchange between MDIS and DSOs CDIS.
5.	Local Area Network (LAN)	Information exchange between the web-based customer interface and CDIS in DSOs internal network.
6.	Extranet / VPN	Information exchange between CDIS and Electricity Retailers billing information system.
7.	Public Internet	Customer monitors own electricity consumption, views billing or sets own information via the customer web-interface provided by the DSO.
8.	Public Internet / manually	Customer requesting the electricity provider to allow a TTP to access his/her consumption data either via web-based customer interface or using a hand written form, telephone or letter.
9.	Extranet / VPN	TTP requesting information from DSOs databases using a private network.
10.	Public Internet	TTP requesting information from DSOs databases via Internet.
11.	Public Internet	Customer monitoring own electricity consumption logs and analyzed consumption data using the web site provided by a TTP.
12.	Manually	Energy regulatory authority doing a information request using either telephone or an official form.

suitable for storing the consumption data for the required time period. These, however, bring risks of their own into play; distribution means that the attackers have multiple targets to attack and multiple communications to eavesdrop. If, for example, the system security upgrades fail for some reason or are delayed by, e.g., network error the attackers might be able to penetrate into the un-protected system during this period and install, e.g., a rootkit to gain access in the future. The content of the distributed databases and the links between different nodes must be properly secured to protect the data. Also the possible in-security of one node should not affect the security of any other node in the distributed database network. The top threats against cloud computing systems are identified by Cloud Security Alliance in [9]. These threats include insecurity of APIs for cloud computing systems, insider attacks and data leakage to name but a few. Analysis of the threats against cloud computing solutions is out of scope of this paper.

One possible solution, which also supports could computing, could be that the data is properly distributed among servers (which is already done with cloud computing); small pieces of consumption data of each customer is spread among the database nodes or into the cloud. If data of all of the customers in certain area is centered on one database node the attacker could target only this node and focus the full arsenal of attacks against it. But if the data is properly distributed the attacker cannot tell which database holds the data of the customers in certain area. Then targeted attacks against the customers in certain area would be no use as the attacker should be able to breach all of the databases in order to gain some valuable information. A solution, which makes it possible to hide the source of the consumption data in plain sight, would be ideal for rendering the data unusable for the attacker. Further discussion about this subject in sixth section.

C. Home environment

In home environment (actors I, I.a, I.b, I.c and I.d using CID 1 and 2 in Figure 2) there is always the possibility that the communication is bound to eavesdropping, tampering of the data or harassing of the household sensors as the communication between appliances is bound to happen over widely used wireless connections e.g. in [5]. Current wireless techniques, e.g. IEEE802.11, Bluetooth or ZigBee, are using omnidirectional antennas which exposes the connections to eavesdropping as anyone in the vicinity can intercept or disrupt the traffic using suitable equipment. In the home environment this would result in leaking of consumption data to malicious users or result in resident harassment if the sensor data is tampered with. There is also a possibility that the attacker could gain access in controlling of some of the household devices, e.g. air conditioning or thermostats. This would be possible if the meters are able to regulate home appliance energy consumption by reducing the temperature of the residence for instance.

Wired network between different appliances would be an ideal solution to prevent unauthorized usage but as the new appliances are needed to be added to the system from time to time it is not practical to revert from wireless to wired connections. To protect the residents from personal information leaks and also from unauthorized usage of their appliances encrypted communication between household appliances is recommended with verification of sent data. Connections and data should be accepted only from authorized devices even in the home environment. The verification of the home appliances and their data was recommended also in [3].

D. Smart Meter access

One of the biggest risks rise on the authoritative usage of the smart meters, as also noted by Anderson and Fuloria in [4]. This includes the tariff changes that are sent to meter, energy consumption data read from the meters and software updates done to meters. Authoritative usage might also include load balancing controlling, which also poses a big risk when the keys are in the wrong hands.

On the connection with CID 3 in Figure 2 the eavesdropping, or data tampering is not such a big issue if a private network is used for data transmission between meters and information systems (as it is done in Finland according to the questionnaire). However, even in this case this should not been taken lightly as the 2G network is not secure [10], [11], nor is 3G [12], not to let alone the rumors that some countries do not even encrypt GPRS traffic[4]. Keeping these things in

[4]http://www.forbes.com/sites/andygreenberg/2011/08/12/codebreaker-karsten-nohl-why-your-phone-is-insecure-by-design/

mind the personal information should be also protected on the mobile network. First good step is to use private networks but the 3G coverage varies in different countries. For example Finland is not fully covered with 3G mobile network [13] so additional encryption must be added. Leaking information here would give too much information about the resident and his/her behavior for the attacker, and giving the easy access to the appliances would be disastrous, therefore, data and authenticity verification is required.

Anderson and Fuloria presented a viable solution for accessing the smart meters using PKI [4] where the manufacturer has the main key, which is used to grant access to the meters. In addition to this it was suggested that each meter has a backup master key in case the original key is compromised. The PKI approach would ensure that the data is sent from verified source and the data is properly encrypted. It would also ensure that only authorized parties can decrypt and access the data. In the case of possible breach of database security or key theft the backup key can be used to gain access to the meter(s) and to replace the compromised key with new one.

E. Company access

The internal communication between information systems of the reader and DSO(s) (via CID 4 in Figure 2) are, or should be, happening through private networks (e.g. VPN, extranet) and, therefore, the risk of eavesdropping is lower. But this scenario brings new threats and risks into play and introduces the weakest link in every security system; employees. Enterprise networks are bound to get attacked quite frequently as the electric espionage is becoming more and more popular. In espionage cases the most effective attack is emerging from inside. Strong and constantly maintained access control system must be used in DSOs information systems to prevent misuse of personal information of the customers [14]. Using an access control system would also protect against possible humane errors that would make impersonation attacks possible. It would not, however, help against attacks coming from outside, e.g., to and via the web-based interface (over CID 5 in Figure 2). But nowadays it is a common procedure to place web-servers in De Militarized Zone (DMZ) to prevent further access into other systems of the corporation [15]. This would bring at least some basic protection if the database access from the web interface is well designed and protected against most common attacks, e.g., SQL (Structured Query Language) injection and other publicly available exploits.

The access to the CDIS from outside should be prevented and only the authorized electricity retailers should be allowed to access it via unified interface (over CID 6 in in Figure 2). The access most likely happens via extranet, VPN or some other closed network, e.g., LANif the electricity retailer and DSO are of the same company and the CDIS might be located in the same corporate network. All of these connections can be classified as secure connections and the risk of eavesdropping is low. The information the electricity retailer requests can be less accurate than the information in the CDIS as only the total electricity consumption of each customer is requested. The risk would be low on this connection and the database breach in the billing information system of the electricity retailer would not threaten the privacy of the customers if they collect only the total amount of the electricity consumed. However, according to [8], in Finland the electricity retailer should get also the hourly consumption data of each consumer. If the data is hourly based the risk on the connection would be higher and it would be classified as the connection between MDIS and CDIS (CID 4 in Figure 2). The total consumption data cannot be used by the attackers but the PII sent along the data can be used for malicious purposes, to connect certain customer to the data for instance.

If the hourly consumption data is shared with electricity retailers it poses a big risk against privacy. The reason is that the same data resides on multiple places and, therefore, attacker can select the weakest one. For this reason all data should be encrypted before subjected to threats of communication networks. When the hourly consumption data is shared with the electricity retailer it would be also necessary to use strong access control systems, as we recommended for the information systems of the DSO. The consumption data stored into information systems of either actor should not be easily connectable to the source of the data, in other words the PII should be separated from the data. This would reduce the threat against customer privacy in case the database security is breached and access to consumption data is gained by the attacker. If the attacker cannot combine the data with the source the data would be useless and, therefore, the privacy of the customers would not be threatened. It would be imperative to allow mapping of data and the PII for those who need it (e.g. DSOs).

The access to the interfaces providing customer information to other parties (DSOs, retailers or TTPs) should be restricted only to the known participants. The connection attempts should be always authenticated and mutual authentication is recommended due to man in the middle attacks (MiTM). With MiTM attacks the attacker could get the authentication credentials when posing as the connection endpoint. The credentials could be then used for accessing the databases of the real connection endpoint. However, if the connections are happening through private networks the risk is much lower but not completely removed.

F. Customer Internet access

Using Internet for revealing personal information is always risky if the connections are not properly secured. The web interface provided by the DSO brings new ways to capture personal information of the customers and to gain access to the consumption data (over CID 7 in Figure 2). The log-in information of the customer can be captured by using, e.g., a phishing attack without actual knowledge of the personal email addresses of the customer. Although there has been lots of warnings about phishing attacks some will still fall for it as the attacks are becoming more professional[5]. This would result in that the attacker could know everything that the DSO knows about the customer. Including the customers energy consumption which can be then used to analyze, for instance,

[5]http://www.f-secure.com/weblog/archives/00002245.html

the presence in the residence [5]. In addition, the attacker could change the personal information through the official web interface and to give access for third parties to the consumption data of that particular customer even without the customer noticing it. To prevent such malicious usage the authentication procedure must be secure and preferably going through an official authentication, e.g. in Finland the authentication via on-line bank services is widely used for verifying identities on-line. However, even strongest encryption does not provide any additional security against phishing attacks as the weakest link is still the same; the customer. To reduce the effectiveness of phishing attacks the DSOs should use the same policy as the banks are currently using; they should not request any personal information nor request the customer to log-in to web interface via email.

In Figure 2 the granting of access for TTPs is represented as CID 8, the access can be granted either electronically via public Internet or by traditional means (a filled form with customers signature). According to the EU directive 2009/72/EC Annex I [2] the consumption data must be given to any registered supply undertaking (which can be intepreted as TTP) if the customer requests it. The requesting of access for third parties to the consumption data of the customer should be made so that the customer always gets a notification about such event. But this is not without risks; this would encourage the attackers to use phishing attacks to send bogus notifications in order to get the customer to log-in with his/her credentials into the phishing site made to look like the company web site. Another much more safe approach is to notify customers with text messages (as they are not free and are less likely to be used by the attackers) or send a notification to the smart meter about such event to avoid potential malicious usage.

G. Trusted Third Party access

The access of the TTP to the CDIS and to the information of a specific customer should be limited and the resolution of the shared consumption data must be reduced to make data mining techniques unusable [5]. TTPs can probably access the public interface of the DSO via Internet (using CID 10 in Figure 2) or via some private network (via CID 9 in Figure 2), e.g. extranet or VPN. In our risk and threat assessment these connections are not the most important ones as the companies decide what information to give to TTPs and which third parties to trust.

But still the risk of using TTPs for analyzing the consumption data of the customers is fairly high. The TTP should in no situation have access to the authentication information of any particular customer on the DSOs systems to avoid the threat of impersonation and identity thefts in case the information system security of is breached. This introduces a big risk in using TTPs; the DSO might not have the possibility to verify the security of the systems used by the TTP and neither has the customer. The connection between DSO and TTP used for transferring consumption data should be always encrypted to avoid eavesdropping. The transferred data should not contain PII or other personal information that can be used to connect a customer to data residing on the database of the DSO.

The TTP should have a different identification information for each customer than the DSO has. For each consumption data request the TTP uses this id which is mapped to the actual customer in the DSOs information systems. The user could be then verified on each log-in to the TTP's web interface via the DSOs systems to check that this identification is connected to the real PII on the DSOs systems. To revoke the rights the DSO could, in addition to blacklisting the TTP in their systems, remove the TTP identification information from the customer information. Another approach in information sharing to TTP is to give the PII along the data that has a resolution so low it is no use for attackers nor it is any use for potentially malicious third party. However, the PII should be always encrypted to avoid potential misuse of the information.

As mentioned earlier, the customer should always get a notification from DSO that access has granted for a TTP to access his/her consumption data. For each data request this might not be necessary hence the phishing attacks but every event when the TTP is requesting consumption data should be logged and available on the web interface.

H. Customer access to Trusted Third Party

The biggest risk in using TTPs is that the information systems of the TTP are attacked and the customer long term information gets stolen. It could be then used for determining, e.g. when the residents are on vacation as there should be a noticeable drop in electricity consumption. The usage of the web interface provided by the TTP (over CID 11 in Figure 2) is not seen as risky as accessing the DSOs web interface as the information on TTP server should not be as accurate as on the DSOs server. The log-in is the most risky part, depending on the implementations the log-in credentials could be:

1) the same as on the DSOs system
2) provided by some other authority, e.g. the DSO or on-line banking services
3) provided by the TTP and the user id can be connected to the PII on the DSOs systems.

Each of these are prone to phishing attacks and also to eavesdropping which can be quite effectively removed with proper encryption of the communication. For phishing attacks the same applies as with the DSOs web interface usage.

The first option cannot be recommended in any case, as breaking of either of the credentials gives access to the information on other system. The risk here is that if the credentials can be selected by the customer there is a possibility that the customers select the same password for both so they have to remember only one password. The risk is even higher when the log-in identification is the same. For this reason the credentials should be "cryptographically sound", i.e. the credentials should be generated so that the cracking of the credentials with raw computational power is not cost worthy nor could they be cracked by using rainbow tables (no known words in password). Or if the customer is allowed to select a password routine checks for password strength must be done.

The second option is almost similar than the first one, with an exception that the TTP does have no access to the credentials. The authenticity of the customer is verified via services provided by other authorities, the TTP only gets the information if the identity could be verified. This poses a low

risk towards TTP but, however, requires additional measures to make contracts about this kind of usage, e.g. with banks in different countries. As the companies analyzing the customers consumption data are usually big global corporations this could be seen as a downside from their point of view.

The third one is most likely to be used in the TTP applications as it gives more freedom for both company and the customers. In this the customer could select any password and the breach of the TTPs systems would not generate any additional risks and threats against the privacy of the customer. It would only reveal the low resolution information provided by the electricity company and some information the customer has provided about him/herself.

For these reasons we recommend that either the second or the third presented approach is used for providing access to TTPs systems for customers. Selecting either one is up to the policies of the company providing the analysis service.

I. Energy regulatory authority access

The ERA of the electricity network and market is responsible of monitoring the actions of the participants delivering electricity and monitoring consumption including the security of the electricity grid [2]. This is usually happening via audits and official information requests that are delivered by traditional means; letter, form or telephone (via CID 12 in Figure 2). The risk of impersonation of an ERA is quite high as it might give illegal access for the impersonator to the data located in the internal systems of the companies involved. According to EU directive 2009/72/EC article 30 [2] the ERA can access the accounting data and other commercially sensitive information. . Therefore, the authenticity of the ERA should be carefully verified with every information request. It was recommended in [3] that the ERA is an independent actor and not a government official. In the EU directive 2009/EC/72 article 35 [2] it is stated that the ERA must be legally distinct from any public or private entity. This puts the ERA out of governmental control and, therefore, the impersonation risk is the highest possible, unless protected by law.

J. The result of the analysis

From the results of the previous analysis we can assign different threat levels for each connection and information system in the presented architecture. The connections, information systems and web-interfaces presented in Figure 2 are categorized with a five level threat system similar to Homeland Security Advisory System as the harassment of electric network and appliances connected to it can be classified as cyber terrorism. In our classification we adapted the threat levels to asses the risk of revealing personal information, risk that the information is tampered with and the risk of being a target of some kind of external attack. The different threat levels and description of each are presented in table IV.

These threat levels are assigned for every connection, information system and web-interface based on the result of risk and threat analysis. The assignment of each threat level is show in Table V. Generally the connections between interfaces provided for other parties, e.g., by the DSO are classified with the lowest threat level since the connections from interfaces to the information systems should be always designed to be secure. The usage of Internet for communication is classified with the highest level because of the multiple possible threats against the transferred PII and consumption data. Connections between different actors are assumed to go through private networks and, therefore, are not classified with the highest threat level. Databases are more likely to be the targets of the attacks and therefore all, except the TTP database hence the low grained consumption data, were given either high or severe classification. Web-interfaces provided by different actors can be classified with the same or one step lower threat level as the underlying information system was classified. This is because the threat cannot be higher than with the one of the information system but it can be lower, though, since the information system must not be directly accessible via the web-interface.

Table IV
THREAT LEVELS

Threat level	Description
Low	The risk of information leak, tampering of information and attack probability is fairly low. Protection mechanisms are not mandatory if basic security is implemented into design.
Guarded	The risk of information leak, tampering of information and attack probability is heightened but not a big risk if proper precautions are taken. Use of protection mechanisms by consideration.
Elevated	There exists a probability for attacks, information leaks and information tampering. Basic protection mechanisms are recommended.
High	There is a high probability of an attack and risk of leaking personal information is high. Advanced protection mechanisms are recommended.
Severe	The connection or information system is prone to attacks and risk of leaking personal information is very high. Strong protection mechanisms recommended.

Table V
CLASSIFICATION OF THREATS ON EACH CONNECTION

Type	Id	Threat level
Connection	1.	Elevated
Connection	2.	Guarded
Connection	3.	High
Connection	4.	Elevated
Connection	5.	Elevated
Connection	6.	Severe
Connection	7.	Severe
Connection	8.	Severe
Connection	9.	Elevated
Connection	10.	High
Connection	11.	High
Connection	12.	Severe
Information system	II.a	High
Information system	III.a	Severe
Information system	IV.a	High
Information system	VI.a	Elevated
Web-interface	III.b	High
Web-interface	VI.b	Elevated

From the classification of threat levels on each communication pathway the results of different threats on them in Smart Grid environment can be estimated. Table VI presents the probable results of information capture, loss, manipulation or corruption on each communication pathway.

Table VI
RESULTS OF DIFFERENT THREATS ON EACH COMMUNICATION PATHWAY

CID	Information is captured	Information is lost	Information is manipulated or corrupted
1.	Reveals home appliance usage, presence, etc.	Measurement data is lost, billing might not be complete for the period.	Invalid data for consumption calculations.
2.	Reveals information about the residence (temperature etc.)	Measurement data is lost, meters cannot adjust themselves (e.g. thermostat).	Invalid data for meters which adjust the components, e.g., thermostats
3.	Reveals the consumption data for 24 hour period and the customer PII.	Invalid billing information for the period where data is lost. Smart meters do not have tariff data.	Consumption data is invalid in the MDIS resulting in invalid billing of the customer
4.	Reveals consumption of all of the residences in the request for the requested time period.	CDIS cannot read consumption information, situation is the same as connection to MDIS cannot be established.	Invalid billing of the customer.
5.	Customer and possibly DSOs data is revealed.	Web interface cannot provide the data for the customer who is requesting. User might not be able to log-in to the system.	The customer gets wrong information about the consumption of the residence. Possibly allows access to another customers data.
6.	Customer total consumption is revealed along possible PII of the customer.	Electricity retailer cannot get consumption data of the consumer for the requested time period.	Invalid billing of the customer.
7.	Reveals possible PII, authentication credentials and consumption data of the customer.	The customer cannot temporarily access the web interface.	The customer gets wrong information about the consumption of the residence.
8.	Reveals the authentication credentials and possibly the TTP with whom customer has made contract.	Customer cannot request access for the TTP to the consumption data.	Malicious third party might get access to customers consumption data. Customer could unintentionally give access to the data for other third party.
9.	TTP authentication credentials for CDIS are revealed. Customer consumption data is revealed.	TTP cannot get access to customer consumption data. TTP cannot provide analysis for customer.	TTP cannot get access to the customer consumption data or gets the consumption data of some other customer. TTP provides invalid analysis for the customer.
10.	TTP authentication credentials for CDIS are revealed. Customer consumption data is revealed.	TTP cannot get access to customer consumption data. TTP cannot provide analysis for customer.	TTP cannot get access to the customer consumption data or gets the consumption data of some other customer. TTP provides invalid analysis for the customer.
11.	Reveals the authentication credentials of the customer to the TTP web site and the analyzed long term consumption data.	The customer cannot access to the web site of TTP and/or cannot get the consumption data analysis.	The customer gets wrong consumption analysis.
12.	ERA authentication credentials are stolen (manually).	Request is not fulfilled (e.g. form gets lost).	ERA gets invalid information.

V. TOWARDS A GENERIC MODEL

The presented reference architecture introduces one common model for Smart Grid environment. In previous chapter we presented the threats on each communication pathway and provided some insight about the risks related to storing the data in different places. This reference architecture took characteristics from the model used in Finland but the roles, ownership and location of different actors might be different in different countries. Here the differences and the effect of each on customer privacy are covered.

A. Changing roles of actors

The DSO and the electricity retailer can be the same corporation, in our reference architecture we have used them as separate actors in order to present all possible risks and threats. However, in Finland some of the retailers also distribute electricity to customers, e.g., Vattenfall and Fortum to name but a few, and it is a common model, for instance, in UK. If the retailer also distributes electricity the connection between CDIS and the billing information system would happen via LAN connection for instance, and, therefore, would be less risky as the information systems probably exist in the same network. The threats against customer privacy could emerge only from inside and the data transmissions would not be prone to eavesdropping. When the retailer is also distributing the electricity the customer personal information and all consumption data might be stored on one shared database. Or the content of the database might be distributed among database nodes or the data resides in the cloud. Nevertheless, the access to the contents of the database would happen via single interface or the connections are restricted to the company's address space. This would remove one, potentially risky connection from the architecture and reduce the risks of information leak. But the earlier mentioned risks and threats about espionage and internal attacks still exist. When the same data is shared, even with different resolutions, between multiple databases of different actors the privacy of a customer can be compromised in various places and, therefore, the risk would be lower when all exist within one actor or is controlled by one actor.

It is not certain which actor provides the web interface for the customers. It can be the DSO as mentioned earlier but the electricity retailer can too provide one, or both of them can provide a separate web interfaces for their customers for different purposes. If the electricity retailer acts also as a distributor and uses a shared database (centered, distributed or cloud computing solution) there might be only one web interface provided for customers. This would reduce confusion among customers as only one login would be required. However, the

reader can also provide a separate interface for customers to monitor own consumption data. It would require that the reader either has own database which keeps the data for specified period of time or the reader has access to the database of the DSO for instance. The placement of the web interface is most likely determined by the contracts between different actors in the Smart Grid environment. Regardless of the placement of the web interface the same threats, mentioned in previous section, exist in all. If the reader provides the web interface the most risky option is to get the consumption data from DSO or electricity retailer. The least risky one would be to provide the data directly from the MDIS or alternatively, provide short term data directly from the meters. The reader might not have the capability to keep all the data for the required period of six years and the data provided for customers would be for shorter period than, e.g. the DSO can provide. The DSO has all the data in the database and can provide consumption data over longer periods without additional risks to the ones mentioned in previous section, as no external system needs to be accessed, same applies for the electricity retailer.

The CDIS could be owned by the electricity retailer but the DSO is more permanent in the environment as the electricity can be bought from different retailers. For this reason it can be recommended that the CDIS is owned by the DSO. It would make the changing of the electricity retailer much more fluent in terms of data access. The DSO could grant access to the consumption data only for the time period the contract is made. Or if the new contract replaces the old one, the DSO could revoke the access rights of the previous retailer and grant access to the data for the new retailer onwards from the starting date of the new contract. This would also increase the customer privacy as data from different periods is not scattered amongst many databases. Since the reader is a separate entity who manages the reading of the data from the meters, there is no need to do any complex ownership changes related to the smart meters. But the tricky part might come when the DSO and the retailer are of same company. If the information systems of the DSO and the retailer are the same and shared database is used it might not be trivial to allow some other retailer to gain access to the customers consumption data and to prevent the access of the "own" retailer to that data. Here comes the problem with distributed data; who owns, who stores and who has access. The customer of course, as stated in [2], owns the data collected from his/her residence and the DSO stores the data for the customer. But the access in this kind of situation would require that the database and the information system used by DSO is separate from the ones used by retailers if they are both the same company. It would be also easier to protect the privacy by disallowing the access to the consumption data of that customer, who has changed the electricity retailer.

In some cases, e.g., in UK and NZ the retailer is responsible for reading the meters. For privacy this is a good thing since the consumption data is not spread among different databases but the changing of electricity retailer might be cumbersome. In our model the reader is assumed to be the telecommunications operator but it does not necessarily need to be one. The reader has to provide an infrastructure for communications between the MDIS and the smart meters and, of course, the reading infrastructure, which includes the MDIS and access for DSOs and/or retailers. The reader could, e.g., use a sub-contractor who provides the communication infrastructure, the most likely choice for the task would be some telecommunications operator. The risks of using an external actor for reading the meters are same as specified in previous section for the reader. However, another actor (the sub-contractor) could introduce new risks if new databases are required to be added into the system.

The actor that provides the data for the TTPs is yet uncertain, the most logical place for this would be the actor that stores all information; the DSO. But, depending on the implementation, it can be the reader, the electricity company or the TTP could access the smart meters directly as it was used as an option in [6]. The access to the information systems, as depicted in the reference architecture, is happening via some specialized interface. The direct access to the meters could be somewhat risky as the TTP could have only the public Internet as an option for accessing the meters. If the problem with unreliable communication pathway could be solved and the access to the smart meters could be done with support of access control lists supporting different access levels, then the threat can be minimized, otherwise the risk of compromising customer privacy is high. The proposed PKI architecture for smart meters [4] could be utilized to grant direct access to the meters for TTPs.

B. Connections between actors

As the roles of different actors can change the connections between them are also implementation dependent. In our reference architecture we presented the most common connection types between the actors. The type of the connection used also affects greatly to the security of the system. The connections happening via public networks can be generally considered as more risky than connections over private networks.

The reading and controlling of the meters can be done via any possible network that is available, the tasks are not connection dependent. As mentioned earlier, wired connections are more secure than wireless ones by nature but are also less flexible. Therefore, the selection of the proper communication technique is up to the reading/controlling service provider. However, as the range of devices utilizing commercial wireless techniques (e.g. mobile phones) is continuously increasing the availability might decrease if the total capacity of the networks is not increased as well. With mobile phone networks the capacity of the base stations might be a limiting factor and with other, widely used wireless techniques, IEEE802.11 (Wireless Local Area Network) for instance, the limited bandwidth is an issue. For this reason, wired connections over private networks might perform better and be less faulty. In order to reduce the interference from public networks and to be available at all times we suggest the usage of private networks with either, wired or mobile networks when communicating to the smart meters. The usage of private networks also reduces the threats against privacy as the transferred data can be well protected. The availability of addresses for each smart meter or for the modem it is connected to should not be a problem as soon as IPv6 is fully utilized in communication networks.

Connectivity between the DSO, the electricity retailer and the TTP is assumed to happen via private networks in the reference architecture. If the information systems used by different actors are in separate locations extranet and VPN are viable solutions as they are properly secured. In case the DSO and the electricity retailer are of the same company the communication between the information systems would happen via intranet connections (e.g. LAN). It is highly unlikely that the corporate actors exchange customer information via public networks but the TTPs could access the consumption data over public Internet. This could be the case when the analysis services provided by multiple different parties are widely emerging and, e.g. the DSO specifies a generic interface for the TTPs to get the needed information.

VI. Potential approach for enhancing privacy

The privacy of the customer can be threatened on different communication pathways by intercepting the transmissions or by breaking into databases storing the transmitted information. The biggest risks lie in the data stored in vast databases as there are multiple victims at stake but the communication between different devices is not without risks. Here we present a possible approach to address the issue in Smart Grid environment or similar architectures.

As the customers PII is sent along the measurement data to identify the source of the data, it is prone to capture and interception attacks and attacks against databases storing the consumption data. Especially if the PII would contain any personal information, but according to the questionnaire, at least in Finland this issue does not need to be worried about as the PII is usually the serial number of the device or IP address used by the device. In few cases the location of the device is used as PII. However, this should not been taken lightly, malicious users could use e.g. data mining techniques to reveal resident activity in certain household [5] if enough metering data is captured. In Finland this might pose a fairly high risk as the whole country is not yet covered with 3G mobile network and in many places only 2G or 2.5G is available [13]. The encryption used in 2G networks has been proved to be inadequate [10], [11]. On the other hand the security of the used communication technique should not be relied on but the flaws and possible risks should be noted and taken care of in the design of the system.

In order to guarantee the privacy of the customers it would be important to not to allow the attacker to know where the captured data originated from. Nor this should be deductable from large quantities of captured data with IP address information. Therefore, we propose to use a solution that hides the PII in the databases and on the communication pathway, starting from the source of the data and ending to the actual database where the PII is required. In the reference architecture the source of the data is the smart meter located in the residence and the end point is the DSOs CDIS. The reader in between does not need this information in any of its operations. In one example approach the PIIs could be pseudorandom and valid only for some period of time. The changing and random PIIs, or One-Time Pseudo Identities (OTPI) for this purpose could be created with a system similar to some One-Time Password (OTP) [16] system.

The benefits this approach gives are very beneficial when the privacy of the customer is at stake. If OTPIs are used there is no risk if the data is captured on the communication pathway or database security is breached. Not even big amounts of captured data benefit the attacker as the source cannot be connected to the data. This would, however, require that the methods for creating the OTPIs are secure and the the future OTPIs cannot be determined from previous, possibly captured OTPIs. So the requirements for the system that creates OTPIs are almost similar as the ones for OTP systems [16].

Additionally this kind of solution would undermine the usefulness of the attacks against the database spread into the cloud or if the database is distributed amongst multiple database nodes. The attacker would have to find a way to connect large quantities of data into unknown user identities and this would require vast amounts of computational power even when a reverse-engineered algorithm is used. The cost of the resource consumption might be even greater than the benefit the stolen information provides for the attacker.

With our proposed solution the development of a standard for communication and data interchange in Smart Grid could begin. This solution would integrate the customer privacy into the design and potentially increase the acceptability of the system among customers. The full analysis of the suitability of the approach for the requirements in Smart Grid environment is beyond the scope of this paper and will be conducted in the future work. In the future research we concentrate on the applicability of the presented solution into Smart Grid environment. The analysis presented in this paper provided valuable guidelines for the future study of the subject about protecting the customer privacy in Smart Grid environment as no such solution exists.

VII. Conclusion

The architecture for Smart Grid environment is quite diverge and there exists no common model to be used for, e.g., analyzing the potential risks against privacy and the security threats. From pilot projects and mapping of current situation an model was derived to help in this kind of task. The abstract architecture contains the different tasks divided into their basics along the basic information flow in the environment but takes no stance on the connections between different actors executing the specified tasks. The abstract architecture was used with the help of previous results (pilots and questionnaire) to form a reference architecture that shows the connections between actors and provides a concrete example about how the different tasks of the abstract architecture are mapped to actors. Since the reference architecture contains only the most generic model, the possible actor role and task changes were introduced and their effect on privacy was presented.

The reference architecture provided a real world situation that could be used for analyzing the potential risks and threats against privacy. In this paper an evaluation of these risks and threats related to connections between different actors in the Smart Grid environment and also the risks and threats against

the information systems storing the data was provided. From the results of the analysis we have derived different threat levels for connections and information systems. The different threat levels were assigned to every presented connection and information system in the reference architecture. With the described method different architectures can be evaluated as the same problems exist in all.

For enhancing the privacy of the customers in the Smart Grid environment a potential approach was presented. The approach aims to protect the privacy with changing identities that are used for each transferred consumption data. Main idea is to create the identities with a system similar to OTP and the changing identities are known only by the source and the collector of data. These identities would render the captured or stolen consumption data unusable for the attacker as the data cannot be tied to certain customer. This approach and the presented reference architecture gives the basis for the future work. In future research the main point is to concentrate on the presented potential approach for enhancing the privacy of the customers in systems similar to the Smart Grid environment. Idea is to develop a secure but flexible method for creating pseudorandom identities for each transferred data in a way that the captured data cannot be connected to any known source by the attacker. The solution will be developed using the guidelines given by OTP approach and its current implementations, challenges presented by the Smart Grid environment and taking account of the flexibility aspect by keeping the cloud computing solutions and distributed databases in mind.

REFERENCES

[1] B. Greveler, Ulrich. Justus and D. Loehr, "Multimedia content identification through smart meter power usage profiles," in *Proceedings of the Computers, Privacy and Data Protection (CPDP) 2012*, pp. x–y, 2012.

[2] European Parliament and Council, "Directive 2009/72/EC concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC," 2009.

[3] R. Anderson and S. Fuloria, "On the security economics of electricity metering," in *WEIS 2010, The Ninth Workshop on the Economics of Information Security*, pp. xx – yy, jun. 2010.

[4] R. Anderson and S. Fuloria, "Who controls the off switch?," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pp. 96 –101, oct. 2010.

[5] M. Lisovich and S. Wicker, "Privacy concerns in upcoming residential and commercial demand-response systems," in *2008 Clemson University Power Systems Conference*, Clemson University, March 2008.

[6] A. Sievi, "Vattenfallin automaattinen sähkönmittaus Suomessa (Automatic electricity metering of Vattenfall in Finland, in Finnish)," in *Adato energy seminar*, 2008.

[7] M. Oy, "Helsingissä panostetaan etäluentaan (Helsinki invests in smart metering, in Finnish)," January 2008. Available: www.mitox.fi/pdf/Lukema0801.pdf.

[8] Finnish Council of State, "Valtioneuvoston asetus sähköntoimitusten selvityksestä ja mittauksesta (Government decree on settlement and metering of electricity deliveries, in Finnish)," 2009.

[9] Cloud Security Alliance, "Top Threats to Cloud Computing V1.0," 2010. Online, Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[10] P. S. Pagliusi, "A contemporary foreword on gsm security," in *Proceedings of the International Conference on Infrastructure Security*, InfraSec '02, (London, UK, UK), pp. 129–144, Springer-Verlag, 2002.

[11] D. Hulton, "Intercepting GSM Traffic." Presentation at Shmoocon 4, February 2008.

[12] U. Meyer and S. Wetzel, "A man-in-the-middle attack on UMTS," in *Proceedings of the 3rd ACM workshop on Wireless security*, WiSe '04, (New York, NY, USA), pp. 90–97, ACM, 2004.

[13] European Communications Engineering, "Operaattorivertailu: Selvitys Suomessa toimivien 3G-matkaviestinverkkojen kuuluvuudesta ja datanopeudesta (Comparison of telecommunication operators: Exploration of the 3G mobile network availability and data speeds in Finland, in Finnish)." Online, 2011. Available: http://www.eceltd.com/3G-verkkojen_vertailututkimus-Kevat_2011.pdf.

[14] X. Huang, H. Wang, Z. Chen, and J. Lin, "A context, rule and role-based access control model in enterprise pervasive computing environment," in *Pervasive Computing and Applications, 2006 1st International Symposium on*, pp. 497–502, aug. 2006.

[15] J. M. Kizza, *Computer Network Security*. Springer, 2005.

[16] N. Haller, C. Metz, P. Nesser, and M. Straw, "RFC 2289: A One-Time Password System," Feb. 1998.