A privacy-preserving Concept for Smart Grids

Ronald Petrlic
Universität Paderborn
AG Sicherheit in Netzwerken
Fürstenallee 11
33102 Paderborn
ronald.petrlic@uni-paderborn.de

Abstract

The *smart grid* is seen as the greatest technological invention — in the context of energy supply — since the grid connection of millions of households. *Smart metering*, as the enabling technology for the future grid, attracts attention of industry, politics, and the scientific community. As smart meters are spreading into more and more households, electricity customers are directly affected by the technology. At the same time, critical voices accuse smart metering of violating customers' privacy. Personal data are collected, allowing electricity service providers a monitoring of customers' habits.

In this paper, we propose a solution that provides anonymity for customers towards their ESP. At the same time, we do not limit the functionality that the ESP is asking for, especially the periodic reporting of customers' current electricity consumption values. Moreover, our concept allows for the ESP to build trust in the software that is executed within their customers' smart meters.

1 Introduction

1.1 Towards a Smarter Grid

Existing mains power supplies, or *grids* for short, are more and more modernized by the introduction of digital systems worldwide. Those systems promise better electricity utilization plannings for *Electricity Service Providers* (ESPs) on the one hand and lower prices for consumers on the other hand. The enabling technology behind this so-called *Smart Grid* is primarily made up by an *Advanced Metering Infrastructure* (AMI). The next step towards "smart homes" is the incorporation of this technology in conjunction with *Building Automation Systems* (BASs) that make use of the provided information in a *demand response* fashion.

In the past, every household had its electro-mechanic analog meter that displayed the electricity consumption. The actual values were typically reported towards the ESP once a year in order for the ESP to charge the customers. The manipulation of meters and thus, electricity theft, was prevented by tamper-evident sealings and locks. The widespread availability of digital embedded devices and low cost communication have made the deployment of smart meters possible. *Berg Insight* estimates that by 2015, 302.5 millions of those devices will be installed worldwide. [4] Politics is also driving the deployment of smart meters. In Germany, measuring point providers are obligated by law (Section 21b, Subsection 3a Energiewirtschaftsgesetz (EnWG) [6]) to provide smart meters in newly built private houses and in private homes that are renovated since January 2010. On the other hand, ESPs are obligated to provide customers a tariff that stimulates energy conservation or the control of energy consumption by the end of 2010 (Section 40, Subsection 3 EnWG [6]). ESPs hope to benefit from cost reductions as they do not have to send technicians to the households to read the meters but let the smart meters report their current consumption values periodically (automated meter reading). Knowing the customers' *current* electricity consumptions can also help the ESPs to better plan their electricity load distribution. On the one hand, there are certain *peak* times when lots of households demand for more electricity and on the other hand, ESPs are facing supply fluctuations. During those peak times, ESPs mostly have to resort to *non*-renewable energy resources. As collapses of electricity infrastructures — e.g. the U.S. blackout of 2003 [1] — have shown, ESPs have to do a profound distribution planning to sustain a high availability and reliability of electricity provisioning. Smart meters involve another benefit in the context of *demand response* electricity utilization. ESPs can provide their customers with up-to-date prices and thus, control the customers' electricity consumption behavior as they are expected to use electricity in times where the prices are low. BASs can make good use of smart grids and automate the electricity utilization of households via smart appliances.

However, smart meters involve some severe *security* and *privacy* challenges. From a security point of view, *electricity theft* is one of the major concerns of the ESPs. As smart meters are basically commodity embedded devices that use "standard" communication technology to report consumption values to the ESPs, they are vulnerable to a wide range of attacks. Our focus in this context is on preserving the integrity of the devices. Furthermore, *authenticity* and *confidentiality* of data must be preserved. On the other hand, from a privacy point of view, we focus on how customers can *anonymously* report their up-to-date electricity consumption to their ESP. We demand that the ESPs must not be able to gain information about their customers' habits based on their electricity utilization patterns. The risk that the electricity consumption profile can be used to draw conclusions about customers habits was pointed out in a report [14] to the *Colorado Public Utilities Commission* and by LISOVICH, ET. AL [10] as well. According to a survey report [2] of the ULD (*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*), the data collected by smart meters are *personal* and allow for a disclosure of personal and factual living conditions of users.

1.2 Electricity Market Architecture

In 1996, the foundation for a liberalised European electricity market was laid by the directive 96/92/EC of the European Union. The goal was to break down the monopoly positions of the ESPs and let the customers choose their ESP more freely instead. This lead to a separation between *grid operators* and ESPs. The grid operator, which cannot be chosen by the customer, operates the grid within a regional area. For the provisioning of its infrastructure, the grid operator gets paid by the ESP. In order to prevent unequably charges, the European Union requested to set up national regulatory authorities that regulate those charges — in Germany, this is the *Bundesnetzagentur*. Moreover, Section 21b of the EnWG also allows for the customer to choose a third-party measuring point provider. However, this is not so common today and thus, in the remainder of this paper, we assume that the grid operator is also the measuring point provider — as it was the case before the liberalisation of the electricity market as well.

The grid infrastructure that is provided by the grid operator is particularly constituted by the site current transformers (CTs) and the switchyards. A site CT typically supplies some tens or hundreds of households. The site CTs are connected to a switchyard. A switchyard serves dozens of site CTs, i.e. a switchyard is responsible for a city. Furthermore, the switchyards are connected to the high voltage switchboards.

1.3 Trusted Computing

In this paper, we come up with a concept for smart metering that takes both, security and privacy, into account. As digital systems are vulnerable to software attacks that cannot be prevented by hardware sealings or solely by means of software, our concept is based on *Trusted Computing*. The grid operator as well as the ESP can build their *trust* in a *Trusted Platform Module* (TPM) as a tamper-resistant device. The grid operator needs assurance that the code executed on the smart meter is *authentic* and has not been tampered with by a customer, or by any other party. This can be achieved by storing a cryptographic hash value of the executed software within one of the TPM's so-called *platform configuration registers* (PCRs). As the smart meter is challenged by an external verifier to attest its integrity, the hash value is signed within the TPM and sent to the verifier. This process is called *remote attestation* and is explained in more detail in [13].

The remainder of this paper is structured as follows. In Section 2, we cover related work. The requirements for a smart grid that preserves privacy are covered in Section 3 and the concept is presented in Section 4. We evaluate our concept in Section 5, before we draw a conclusion and give an outlook in Section 6.

2 Related Work

There are several research papers that focus on security in the context of smart metering. Most authors assume that the customers are the attackers that want to steal electricity.

McLaughlin, Podkuiko, and McDaniel [12] perform a profound security analysis for the AMI. They also point out that the smart meters are vulnerable to (software) manipulations and that the network links constitute particular points of attack.

LeMay, Gross, Gunter, and Garg [9] were the first who proposed to employ TPMs within smart meters. The main purpose of the TPM in their concept is the authentic report towards the ESP that the software executed on a smart meter has not been tampered with. The

ESP needs assurance of this fact as the smart meter's software is responsible for the calculation of the customer's monthly bill. However, the authors pointed out that TPMs are not best suited for their purpose as those devices' power consumption is too high in idle mode — under the assumption that the TPM is used for remote attestation once a month. Thus, they came up with another approach towards building trust in embedded devices in [8].

In the context of privacy preservation, BOHLI, SORGE, AND UGUS [5] were the first who presented a solution where the ESPs are not aware of up-to-date information about electricity consumptions of individual customers but rather of groups of customers and thus, preserving the individuals' privacy. The main difference to their paper is that we neither require a trusted third party as an aggregation proxy that is involved in each meter reading and that has to keep track of those data — together with the identity — to be able to bring to account the utilization at the end of a year, nor do we add random values to the meter reading values.

Another privacy-preserving approach has been suggested by GARCIA AND JACOBS [7]. They suggest to use homomorphic encryption to prevent the ESP from gaining consumption data of individual households.

3 Requirements concerning the Smart Grid

In this section we work out the security and privacy requirements that have to be met by a smart grid. Therefore, first of all, we cover the requirements from a technical point of view before we point out non-functional requirements and security and privacy requirements in the last step.

3.1 Functional Requirements

Smart meters constitute the main components in the smart grid. Beyond *data collection* and *data processing*, we primarily focus on the communication of smart meters with different parties, which are particularly the ESP, the grid operator, and the customer in this examination.

3.1.1 Smart Meter - ESP

Periodically reporting the electricity consumption data towards the ESP is a major functional requirement for smart meters. In state of the art implementations, the typical interval is a quarter of an hour. Those data allow the ESP to better plan the electricity load balancing. Furthermore, the ESP needs data from the smart meter to bill the customer for the electricity provisioning. Note that billing on a monthly basis — rather than per annum — is preferred by customers and is also supported by law (Section 40, Subsection 3 EnWG [6]).

Another important requirement is up-to-date price information provided by the ESP. In conjunction with a smart appliance, this enables the customer to save money as electricity may be primarily consumed when the price is low. The policies for the smart appliance have to be specified by the customer, e.g. via a web interface. On the other hand, ESPs could demand that the approach is not customer-centric but rather controlled by themselves. Therefore, the ESP needs a feedback channel towards the customers' households to be able to put devices that draw a lot of energy, e.g. air conditioning systems, out of operation. The customers' smart appliances have to incorporate the ability to receive and execute such commands provided by the ESP.

3.1.2 Smart Meter - Grid Operator

The grid operator needs the consumption data from customers to charge the ESP for the provision of its infrastructure. Thus, the smart meter has to provide the grid operator with those data.

Moreover, the grid operator must have the possibility to remotely update the smart meters' software. For example, if a bug in the software is found, a quick update of the software is needed in order to prevent the exploitation of the security vulnerability.

3.1.3 Smart Meter - Customer

The smart meter should also provide an interface that allows the customer to get an overview about the current electricity consumption. The matching with currently running devices allows the customer to keep track of how much electricity is drawn by each device. The resolution of the utilization data should be in the range of a second to yield a profound live analysis.

There already exists such a solution, which is called *PowerMeter* [3] and is hosted by *Google*. Customers have to send their consumption data to Google and they are presented a graphical visualization of the data that allows them to keep track of the current electricity utilization of their devices. We do not want to rely on a third party to provide that service.

3.2 Non-Functional Requirements

Smart meters have to be permanently *available* and *reliable* as the ESP depends on the up-to-date electricity utilization data and on the correct computation of the monthly bill. The smart grid is expected to constantly grow very fast and thus, it should be *scalable* as well. In particular, authorities that are needed, e.g. the trusted third party (TTP) as presented in Section 4, must not constitute the bottleneck.

3.3 Security and Privacy Requirements

Security and privacy requirements can be split up according to the different parties in the smart grid. The ESP requires the current consumption data for the utilization planning as well as the monthly bill to be authentic. Those data are originating from the customer who needs to stay anonymous at the same time. Moreover, the grid operator takes a particular position in terms of trustworthiness.

3.3.1 Security from the ESP's point of view

For the ESP, the most important protection goal is the *authenticity* of the monthly bill that is computed by the customer. However, the customer is not trustworthy from the ESP's point of view — the customer is assumed to manipulate the meter readings or the computed bill. Analog meters could be attacked by mechanical manipulations, e.g. through meter inversion. Smart meters do not allow such attacks but they are rather vulnerable to more problematic attacks, i.e. software manipulations and the modification of consumption data by means of network attacks. An attacker who is able to reprogram the software that is executed on the smart meter, e.g. by employing the remote update mechanism, can modify the code that is used for the calculation of the monthly bill. The challenge for the ESP is that there is no chance to trust the computation performed by the smart meter as this commodity device does not constitute a trustworthy device — after all, it is not sure whether the computation is performed on the smart meter or on a standard PC. Thus, software integrity is a major requirement on the part of the ESP. Furthermore, the calculation of the bill within the smart meter requires the price information provided by the ESP to be authentic and not to originate from the customer who lowers the price this way.

Another threat that targets the smart grid is terrorism. Smart appliances accepting non-authenticated price information could be employed to create an excess demand of electricity by providing a minimal price to a large amount of customers and thus, causing a breakdown of the grid. Non-authenticated commands sent to smart meters even constitute a more severe problem in the context of keeping the availability of the grid.

3.3.2 Privacy from the Customer's point of view

From a customer's point of view, the protection goal *anonymity* is the most important one. We require that no party — not even the ESP — may be able to link consumption data to any individual customers. Moreover, we require the ESP not to be able to create an electricity utilization profile under a pseudonym. This would allow for a linking of a pseudonym to a customer at the end of a month when the ESP receives the bill, which bears identity information of the customer. For an ESP to be able to better plan the needed electricity, it is crucial — and sufficient — to have utilization statistics about a *coarse-grained group of households*, e.g. within a certain regional area.

As we have pointed out, we require the user to be able to graphically visualize the current power consumption of devices in operation. The state of the art service hosted by Google that provides this functionality entails the potential to violate the privacy as the customer cannot know what Google uses those data for. For example, in conjunction with a *Google Calendar* used by the customer, Google could map electricity consumption data to the information stored in the calendar, allowing for a better derivation of customers' current activities. Thus, we require the processing of consumption data to be done within the customer's premises.

3.3.3 Trustworthy Grid Operator

Customers and the ESP both have to trust the grid operator. The customer cannot appear anonymously towards the grid operator but rather appears under a pseudonym — the grid operator should not know the full identity but only know the household of the customer. The customer needs to trust the grid operator to withhold the customer's pseudonym when forwarding consumption data towards the ESP. At the same time, the ESP needs to trust the grid operator as well, namely that the grid operator checked the authenticity of the data received by customers. Moreover, the ESP has to count on software integrity checks performed by the grid operator in order to be able to know that the bill computation has been done correctly by the customer.

4 Concept

In this section we present our concept of a smart grid in which the primary goal is the preservation of the user's privacy. We propose a smart grid architecture in Section 4.1. The initialization phase that is needed to set up a smart meter as proposed with our concept is covered in Section 4.2. Privacy-preserving data provisioning is presented in Section 4.3 and an approach of electricity consumption control is covered in Section 4.4. In Section 4.5 and Section 4.6 we discuss the integrity attestation of the smart meter and the bill computation.

4.1 Smart Grid Architecture

Each household is equipped with a smart metering device whose purpose is the collection of electricity consumption data for the provisioning of up-to-date data towards the ESP in short-term intervals, e.g. every quarter of an hour, and the local computation of the monthly bill within the device. By employing trusted platform modules (TPMs) within the smart meters, we can make use of software integrity attestation on the one hand, and allow for a unique identification as well as pseudonymisation during the provision of electricity consumption data on the other hand. A unique identification of a TPM is provided by an endorsement key (EK) certificate and pseudonymisation can be achieved by the utilisation of a pseudonymous credential issued by a trusted third party (TTP).

The architecture we propose for an integration of the smart meters to the smart grid is shown in Figure 1. All the data from the smart meters, consumption data as well as bills, have to be sent to the ESP in some way. However, a direct connection, e.g. based on the *Internet Protocol* (IP), would release address information (IP address) to the ESP and allow for an identification again — in spite of pseudonymisation applied on application level. We propose the following network architecture. The smart meters of the households are connected to the site current transformer (CT) in a star-topology-organized network using Powerline Communication (PLC) as a shared broadcast medium. Note that we suggest PLC mainly for reasons of practicability — e.g., DSL or WiMAX would also constitute possible network access technologies, however, requiring (more expensive) equipment that might not be present, e.g. DSL lines or WiMAX base stations. The site CTs are furthermore connected to a switchyard and the

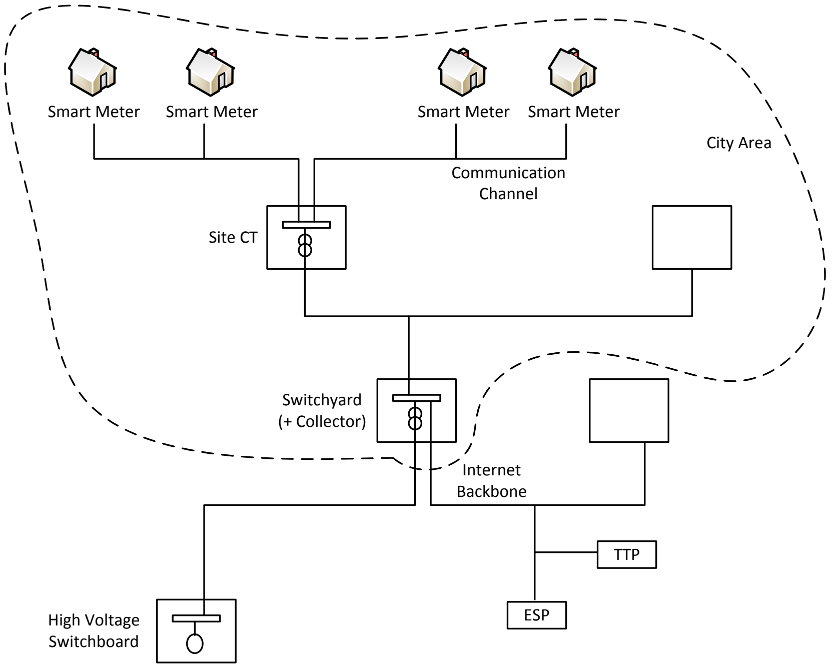

Figure 1: Smart Grid Architecture

switchyard is in turn connected to the Internet backbone. Thus, the switchyards act as proxies between the households and the ESP that is also connected to the Internet backbone. Thereby, we can prevent the ESP from identifying a household based on its IP address. We propose collectors, which are part of the switchyards, that forward the data from the households with their own IP address as source address and thus, the ESP can relate the received data only to a certain regional area. We further propose that a TTP, which is also connected to the Internet backbone, is managed by the national electricity regulatory authority. In Section 1.2, we pointed out that the grid operator and the ESP are generally independent parties and we require the grid operator — more precisely, the collector node operated by the grid operator — to be a trustworthy party in Section 3.3.

Next, we cover the tasks that are executed in order to realize the requirements as stated in Section 3. The *initialization* is performed when a new customer takes control of a smart meter. *Data Provisioning*, *integrity attestation*, and *bill computation* are periodically performed tasks. All of the tasks mentioned so far are initiated by the smart meter. *Electricity Consumption Control*, on the other hand, is initiated by the ESP — performed non-periodically.

4.2 Initialization

The smart meters are provided by the grid operator. As each smart meter is equipped with a unique EK certificate, the grid operator has to keep track of which device is supplied to which household. The grid operator also has to provide the TTP with all the valid EK certificate serial numbers in order for the TTP to issue credentials only for valid smart meters. The initialization phase is shown in Figure 2.

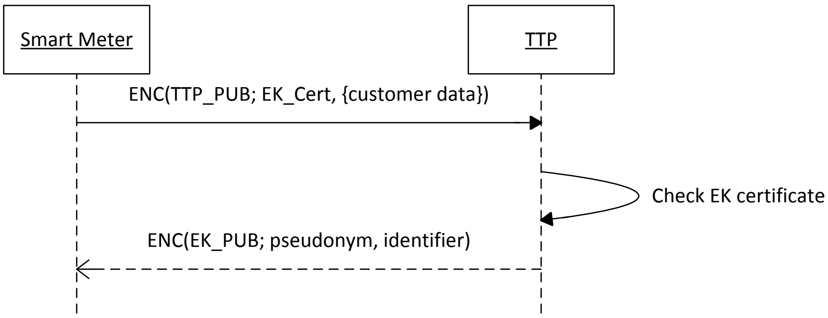
Smart Meter
TTP
ENC(TTP_PUB; EK_Cert, {customer data})
Check EK certificate
ENC(EK_PUB; pseudonym, identifier)

Figure 2: Initialization Phase

As a smart meter is taken over by a new customer at a household, the first task is the identification of the smart meter and the customer by the TTP. Therefore, the smart meter sends its EK certificate and the customer's personal data to the TTP. The customer's personal data can be provided to the smart meter via a web interface. The ESP provides the new customer with a PIN to acknowledge the transaction. As the grid operator must not learn the customer's personal data, the request is encrypted with the TTP's public key. The TTP checks whether the request comes from a valid smart meter and then issues a *pseudonym* and an *identifier*. Each of them consists of a key pair and a signed certificate. Thus, we get the following: *pseudonym = (PS_PRIV, SIG(TTP_PRIV; PS_Cert))*, where *PS_PRIV* denotes the private key of the pseudonym and *SIG(TTP_PRIV; PS_Cert)* means that the pseudonym certificate *PS_Cert*, which also includes the corresponding public key *PS_PUB*, is signed with the TTP's private key *TTP_PRIV*.[1] Note that the pseudonym does not contain any personal data of the customer and thus, is not linkable to an individual customer. On the other hand, the TTP also issues the following identifier that contains the customer's personal data within the certificate: *identifier = (ID_PRIV, SIG(TTP_PRIV; ID_Cert))*. The customer's personal data are needed for the monthly billing. The TTP responds to the smart meter with the encrypted pseudonym and identifier: *ENC(EK_PUB; pseudonym, identifier)*. As the message is encrypted with the endorsement key (EK), only the proper smart meter's TPM is able to decrypt the message and receive the credentials.

4.3 Data Provisioning

As we have pointed out in Section 3, the customer is interested in live analysis of consumption data, the ESP is interested in utilization data for load planning, and the grid operator needs the data to charge the customer's ESP for the provisioning of its infrastructure.

4.3.1 Data Provisioning for the User

The provisioning of the "live" data for the user is done by the smart meter's web server — protecting the data via a TLS connection. This protection is necessary as the internal house network access medium might be WLAN or PLC and we do not want neighbors to get access to those data.

[1] We use the same notation for the encryption scheme as well.

4.3.2 Data Provisioning for the ESP

The data provisioning towards the ESP is shown in Figure 3. The averaged consumption data value, over quarter of an hour, is first encrypted with the ESP's public key *ESP_PUB* and then signed within the smart meter's TPM with the pseudonym private key *PS_PRIV*. The result is forwarded to the collector. It is the collector's task to verify the signature. Therefore, the collector needs the pseudonym certificate *PS_Cert*. After the verification, the collector removes the signature and forwards the (encrypted) data towards the ESP. The data have to be authenticated by the collector to prevent any manipulations and the ESP must not accept any data from other parties. For that purpose, we suggest to use a *message authentication code* (MAC) with a shared (symmetric) key between the collector and the ESP (COL-ESP_SK).[2] A MAC is preferable over a digital signature in this case, as a MAC computation can be performed more efficiently — most notably, the collector has to authenticate a huge amount of data values every quarter of an hour. The ESP, which finally decrypts the data, does not know the origin of the data but it can rely upon the data as the collector attests for its authenticity.

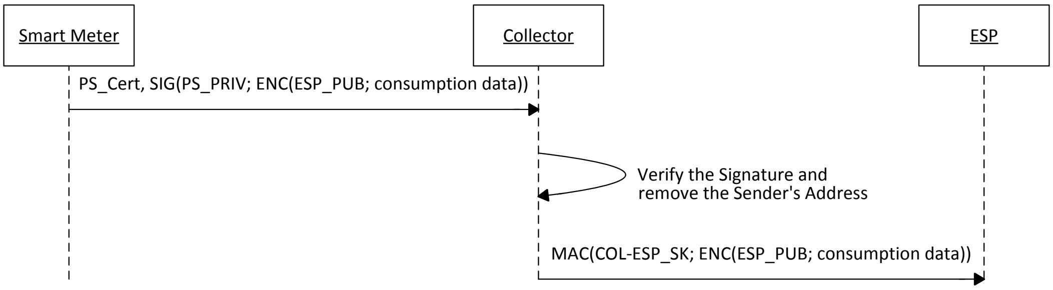
Smart Meter
Collector
ESP
PS_Cert, SIG(PS_PRIV; ENC(ESP_PUB; consumption data))
Verify the Signature and remove the Sender's Address
MAC(COL-ESP_SK; ENC(ESP_PUB; consumption data))

Figure 3: Data Provisioning towards the ESP

4.3.3 Data Provisioning for the Grid Operator

The grid operator needs the information about how much electricity is conveyed through its infrastructure in order to be able to charge the ESP for the provision. For that purpose, the smart meter sends its consumption data signed with the endorsement key to the grid operator once a year. The grid operator can only use this value to charge the ESP — it is not possible to draw any conclusions about the user's habits from this single value.

4.4 Electricity Consumption Control

As the ESP knows about the consumption on a city scale, it can only tell the corresponding switchyard to broadcast a control message within its domain. For example, such a control message could prohibit any household within a city from charging electric vehicles right now. The smart meter forwards this message to the smart appliance and it is the smart appliance's task to stop charging the vehicle if one is present and charging right now.

[2] For a practical implementation, a TLS-channel, which provides, among other things, message authentication, may be used for the communication between the collector and the ESP — provided that mutual authentication is performed.

4.5 Integrity Attestation

Smart meters employ *software* to control the measurement and process the measurement values. The main advantage of a software implementation, in contrast to the use of dedicated hardware, is that the functionality of the smart meter can be extended via (remote) updates without having to exchange all the devices. We have to ensure that only authentic updates from the grid operator are accepted by the smart meter. Therefore, we can implement an update mechanism that only accepts software updates that are digitally signed by the TTP. Having the updates signed by the TTP, and not by the grid operator, simplifies the certificate management within the smart meter on the one hand, and allows for an easier certification of smart metering software by an independent authority on the other hand. However, software implementations are always prone to attacks, e.g. due to programming errors. Thus, an attacker may manage to circumvent the update mechanism and thereby manipulate the software within the smart meter. MCDANIEL ET AL. [11] call this the *Billion-Dollar Bug* in this context. The successful compromise of a smart meter can help customers to save a lot of money, or, on a grand scale, can give terrorists the opportunity to shut down whole cities by sending the smart meters bad commands. We rely on *remote attestation* as covered in Section 1.3 to detect any manipulations of the smart meter software. The grid operator could generate the proper *attestation identity key* (AIK) credential and implement it within the smart meter in advance to its delivery. The AIK credential must also include the address of the household so that further investigations can be initiated in the case of an integrity violation being noticed.

4.6 Bill Computation

For the bill computation to yield correct results, not only the software that performs the computation has to be authentic, but also the actual price information provided by the ESP has to be. This can be achieved by allowing only digitally signed price data for the computation. As the TPM does not provide a sufficient amount of data storage for all the price data and the consumption data, some storage facility within the smart meter, i.e. flash memory, has to be employed. It is crucial that those data are integrity-protected by using a message authentication code with a key that is protected by the TPM and only released for the logging and bill calculation application. We do not require those data to be encrypted as the web server application running on the smart meter should be able to access those data as well, in order to be able to present the customer live information about the electricity consumption and pricing.

In order to keep the communication overhead at a reasonable level, we can assume that the ESP provides the customers with price updates every quarter of an hour. At the end of a month, only a single computed result value is transmitted towards the ESP. However, the customer can check the bill on a daily basis via (local) web access to the smart meter.

5 Evaluation

With our concept presented in this paper we meet all the requirements as requested in Section 3. As we have focused on the privacy of the smart grid, our most important contribution is that we have come up with a solution that introduces anonymity in the provisioning of up-to-date customers' consumption data towards an ESP. Thus, those data that are crucial for the ESP for a more effective utilization planning cannot be linked to individuals any longer. Moreover, the ESP cannot even create a profile under a pseudonym based on the periodic customers' utilization values. At the same time, we achieve this up-to-date provisioning of data without having to increase the intervals between transmissions, as demanded by data protection specialists.

We achieve privacy protection from the ESP as the ESP does not receive the consumption values directly from the smart meters but rather from the grid operator. The grid operator's switchyard appears as a data collector that on the one hand checks the authenticity of the data and on the other hand forwards the data without the signatures with its own source address — authenticated — towards the ESP. As the data can only be linked to a city and the ESP receives only a bill at the end of a month from each customer, the provider is not able to sum up the single data values and compare them to the monthly bills.

The grid operator, which we assumed to be trustworthy, does not have the chance to create a profile under a pseudonym either. The collector node receives the data under a pseudonym directly from the smart meters but as the data are encrypted, the grid operator does not see the data. Thus, even if he receives an aggregated value over the consumption values at the end of a year, he cannot use this information to draw any conclusions from this single value.

The last threat to look at is what happens if the grid operator and the ESP cooperate — in contrast to our assumption that those are independent parties. Again, the same argument as before is true in that case as well. The grid operator gets the sum of the consumption values of a household over a year and in the same period of time, the ESP gets the single consumption values of all households within a certain city from that grid operator every quarter of an hour. Linking those values to the total annual sum of values is practically infeasible as the number of values received from thousands of households every quarter of an hour within a year is too high to be able to relate it to a certain annual sum. Thus, we can assume that an increased sending rate of consumption values would make such a linking even harder as the number of values received over a year gets higher.

Furthermore, our solution is resistant against false data injections as pointed out by LE XIE, ET AL. [15] as all data transmitted towards the ESP are authenticated.

6 Conclusion and Outlook

The main point of critique of the survey report [2] of the ULD against smart metering was that smart meters collect personal information. We came up with a solution that prohibits a linking of consumption data collected by smart meters neither to a certain individual nor to a certain pseudonym. As we do not make any unrealistic assumptions for a smart grid that preserves privacy as we suggest, we have come up with a practical solution that should be taken into account when grid operators expand the smart grid. To further emphasize the practicability of our solution, we want to come up with a prototypical implementation of our concept in the near future.

References

[1] Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. Technical report, U.S.-Canada Power System Outage Task Force, Apr. 2004. `https://reports.energy.gov/BlackoutFinal-Web.pdf`.

[2] Datenschutzrechtliche Bewertung des Einsatzes von 'intelligenten' Messeinrichtungen für die Messung von gelieferter Energie (Smart Meter), Sep. 2009. Unabhängiges Zentrum für Datenschutz Schleswig-Holstein.

[3] Google powermeter. Webpage, 2010. `www.google.com/powermeter/`.

[4] Berg Insight. Worldwide installed base of smart electricity meters will reach 302.5 million units in 2015. Webpage, Aug. 2010. `http://www.berginsight.com/News.aspx?s_m=1&m_m=6`.

[5] Jens-Matthias Bohli, Osman Ugus, and Christoph Sorge. A Privacy Model for Smart Metering. In *Proceedings of the First IEEE International Workshop on Smart Grid Communications (in conjunction with IEEE ICC 2010)*, 2010.

[6] Bundesministerium der Justiz. Gesetz über die Elektrizitäts- und Gasversorgung, Jul. 2005. `http://www.gesetze-im-internet.de/bundesrecht/enwg_2005/gesamt.pdf`.

[7] F. D. Garcia and B. Jacobs. Privacy-friendly energy-metering via homomorphic encryption. In *Security and Trust Management (STM 2010)*. Springer, 2010. LNCS.

[8] Carl A. LeMay, Michael andGunter. Cumulative attestation kernels for embedded systems. In *ESORICS*, pages 655–670, 2009.

[9] Michael LeMay, George Gross, Carl A. Gunter, and Sanjam Garg. Unified architecture for large-scale attested metering. In *Hawaii International Conference on System Sciences*, Big Island, Hawaii, Jan. 2007. IEEE.

[10] Mikhail A. Lisovich, Deirdre K. Mulligan, and Stephen B. Wicker. Inferring personal information from demand-response systems. *IEEE Security and Privacy*, 8:11–20, 2010.

[11] Patrick McDaniel and Stephen McLaughlin. Security and privacy challenges in the smart grid. *IEEE Security and Privacy*, 7:75–77, 2009.

[12] Stephen McLaughlin, Dmitry Podkuiko, and Patrick McDaniel. Energy theft in the advanced metering infrastructure, Sep. 2009. In the 4th International Workshop on Critical Information Infrastructure Security.

[13] Thomas Müller. *Trusted Computing Systeme - Konzepte und Anforderungen*. Springer, 2008.

[14] Elias Leake Quinn. Smart Metering & Privacy: Existing Law and Competing Policies. A Report for the Colorado Public Utilities Commission, University Colorado Law School - CEES, May 2009.

[15] L. Xie, Mo Y., and B. Sinopoli. False data injection attacks in electricity markets. In *2010 First International Conference on Smart Grid Communications*, Oct. 2010.