Grant Agreement Number: **248113/O70**

Project acronym: **IoTSec**

Project full title:

Security in IoT for Smart Grids

D2.1.1

Privacy Aware

Due delivery date: M12

Actual delivery date: M41

Organization name of lead participant for this deliverable:

Norwegian Computing Center/Norsk Regnesentral

Dissemination level		
PU	Public	
RE	Restricted to a group specified by the consortium	**X**
CO	Confidential, only for members of the consortium	

Deliverable number:	D 2.1.1
Deliverable responsible:	Habtamu Abie
Work package:	WP2
Editor(s):	Sigurd Eskeland

Author(s)	
Name	**Organisation**
Sigurd Eskeland	NR

Document Revision History			
Version	**Date**	**Modifications Introduced**	
		Modification Reason	**Modified by**
1.0	15.02.2019		

1 ABSTRACT

In this report, we present an overview of privacy-aware models and related measures of privacy for smart meters. A presentation of privacy concepts such as privacy threat actors and privacy threats applicable to smart meters are provided.

Detailed objectives

In this task, we will build privacy-preserving among the key entities in a distributed manner without relying on an online trusted party. We will also design and implement privacy designs for metering and control of grid-connected devices and protocols. In addition, we will carry out privacy impact analysis and deploy user-centric privacy technology. This will

- establish privacy-preserving communication among the customers and the service providers to protect end users' private information
- establish privacy requirements and a security model
- efficiently handle communication failures while ensuring privacy

Specifically, we suggest non-interactive privacy-preserving aggregation, since this avoids the high smart meter communication interaction and encryption overhead quadratic to the number of users. For this task, we will propose and implement a scheme that supports dynamic group management, which thus avoids the disadvantages of full key redistribution of joining and leaving meters. Privacy-preserving billing will be considered if time allows.

2 EXECUTIVE SUMMARY

This document summarizes deliverable D2.1.1 of the IoTSec project (248113/O70), a research project supported by the Research Council of Norway (RCN).

Full information on this project is available online at http://cwi.unik.no/IoTSec:Home

I. TABLE OF CONTENTS

II. TABLE OF FIGURES AND TABLES

3 INTRODUCTION

The purpose of this report is to provide an overview of privacy-preserving schemes for the smart grid/smart metering scenario. A presentation of privacy concepts such as privacy threat actors and privacy threats, which are applicable to smart meters, is provided.

Privacy pertains to individual users and their personal data. Privacy is in essence motivated by the need for protection of personal data, actions, or even identities, such as social security numbers. The need for protection is eventually motivated by someone or something that represents threats to the privacy of an individual. Threat actors include data controllers and data processors, and external parties. Thus, a threat model is assumed. In agreement with this reasoning, we refer to this category of privacy as threat-motivated privacy.

In “classic” energy systems, the power delivery from energy supplier to homes is one-directional in the sense that the electricity is distributed from the power stations through the power distribution network to the end consumers. Such systems give a predictable, controllable and centralised power generation. Grid systems allow several energy sources to be connected to the distribution system, which provide decentralization and add more variables in the system. The smart grid introduces IT systems for communication, sensors and automation. The smart grid is in other words a dynamic system that allows distribution system operators (DSO) to actively manage the varying power generation and demand.

Advanced meter infrastructure (AMI) is an integrated system that measures, collects and analyses energy usage by using smart meters. Smart meters allow two-way communication and automatic fine-grained measurement reporting at short time intervals, e.g., every hour, to the head-end systems of the electricity providers. The two-way communication allows utilities to remotely control smart meters, for instance to remotely cut off electricity supply to households in cases where users have not paid their bills. Hence, security measures are imperative in this context.

It is claimed that fine-grained end-user measurements increase utilities’ and grid operators’ control and monitoring of electric consumption and network loads, i.e., load monitoring and load management, which is not possible with traditional meters. At times when the collective consumption reaches peaks or lows in the distribution networks, it is desirable to smooth the peaks and lows to even the load distributions. Demand response is such a measure for load management, which are programs that offer consumers economic incentives in order to adapt their usage of electricity in response to wholesale market price signals.

In essence, smart meters are deployed because of their ability to provide fine-grained measurements, which provide increased operational control and allows for dynamic billing regimes and flexible pricing models in accordance with hour-to-hour variable tariffs. Moreover, two-way smart meter communication allows utilities to remotely issue commands to smart meters.

4 PRIVACY TAXONOMY

When designing privacy-preserving systems, relevant privacy threats need to be identified. When threats are identified, a set of privacy requirements can be formulated, which correspond with privacy properties that are necessary to protect against the privacy threats.

The concepts of privacy and security are often confused, and it can be useful to point out relevant distinctions. Figure 1 shows what properties pertain to privacy and security. Confidentiality (secrecy) pertain to both.

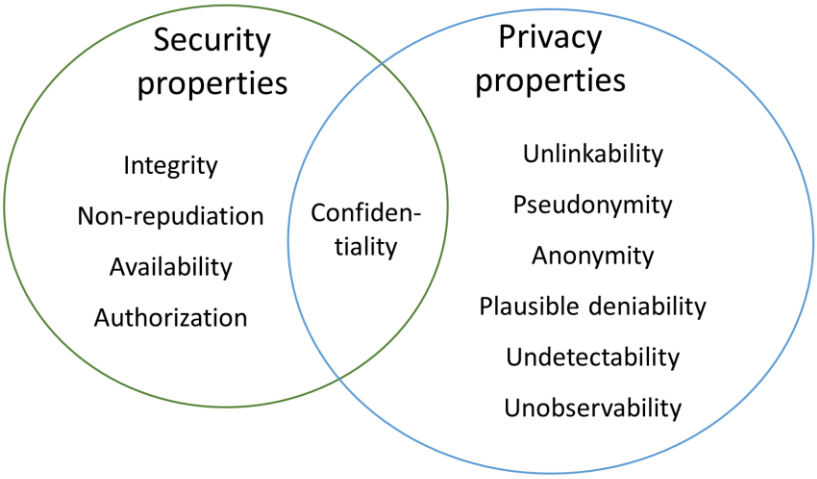

Figure 1. Privacy and security properties

In order to build privacy designs for the smart grid scenario, it is necessary to establish relevant privacy threats and the types of privacy threat actors.

4.1 Privacy threat actors

Threat actors we consider relevant are:

- Honest-but-curious electric utility/distribution system operator (DSO).
- External adversaries

We assume an honest-but-curious utility that do not deviate from the defined protocol, but will attempt to learn all information possible from the received messages. Realtime monitoring and registration of electric usage constitute invasive factors into the privacy of the consumers. From the users' perspective, the utility therefore constitutes a privacy threat actor to the users, since their smart meters are continuously submitting user-sensitive measurement data to the utility.

We will in this task not distinguish between electric utility and DSO, since the users are subject to both and from the user perspective constitute a single privacy threat actor.

Also from the users' perspective, external parties and other users may constitute not only security threats but privacy threats.

From the utility's perspective, users do not represent privacy threats, but rather potential security threats given the possible motivation of cheating the utility. More specifically, an advanced user may be capable to replay former messages or to create valid messages with false consumption values. This is equivalent with an active external adversary that is able to modify messages that are in transmission. However, such threats fall into the category of security threats. Nevertheless, this could be considered.

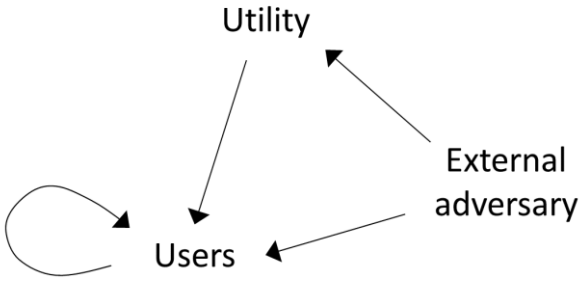

Figure 2. Threat actors and threat targets

4.2 Privacy threats

"Personal data" is a generic term that pertains to data that relate to a person, usually data with a degree of sensitivity. In this context, privacy relates to the relationship between a person, his or her personal data, and how personal data are collected, processed and stored. This includes also what types of personal data are being collected. Privacy also relates to the relationship between a person and actions carried out by that person. For example, the sensitivity of identifying information may depend strongly on context, like the nature of situations it could link a person to.

There is a privacy property for every privacy threat, so that given a privacy threat there exists a privacy property that corresponds to and neutralizes that threat. Table 1 shows a mapping between the privacy properties included in Figure 1 and pertaining privacy threats.

These properties are characterized in Deng (2011) as "hard privacy, and pertain typically to visibility of user data (confidentiality), user/data-relationships (linkability) and user behaviour. Threat models where data controllers and data processers are not trusted are reasonable and common, which lead the user to seek to submit as little personal data as possible and to decouple links between himself and personal data. Privacy measures orient towards user data minimization, increase the abstraction level of user data, and "hiding" user data.

In contrast, "soft privacy" focuses for instance on transparency, intervenability, specific purposes for data processing, user consent, policies and audit. According to Hansen (2012), transparency includes the 1) users' right to access their personal data, 2) information about how this personal data is being processed, 3) for what purposes personal data is being processed, 4) with whom personal data is shared, and 5) how are personal data acquired. Intervenability regards measures for data controllers to effectively control data processors. For data subjects, intervenability includes the right of rectification of incorrect user data, the right to erasure of data ("the right to be forgotten") and the right to withdraw consent.

Privacy threat	Privacy property
Linkability	Unlinkability: Hiding the link between two or more identities, pieces of information or actions.
Identifiability	Anonymity: Unlinkability with regard to subjects: Hiding the link between a user or a user's identity, and a piece of information or an action pertaining to that user. Anonymity can be realized by pseudonyms (pseudonymity), which are identifiers of subjects that are not the real name.
Non-repudiation	Plausible deniability: The ability to deny having performed an action that other parties can neither confirm nor contradict.
Detectability	Undetectability: Hiding of messages and users' activities. Regarding messages, undetectability means that an adversary is not able to distinguish between messages, e.g., from random noise. For example, given only ciphertexts, an adversary is not able to know whether a specific plaintext exists of not.
Information disclosure	Confidentiality: Hiding of data content. According to NIST, confidentiality is preserving authorized restrictions access and disclosure, including means for protecting personal privacy and proprietary information.

Table 1. Privacy threats and properties

Table 2 is included for the sake of completeness, and it shows the relationships between security threats and security properties. Notice that confidentiality can be regarded both as a security property and privacy property. Also, note that the non-repudiation security property is a privacy threat, since this property represents evidence that proves something that a user has said or done.

Security threat	Security property
Unauthorized information disclosure	Confidentiality
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation

Table 2. Security threats and properties

5 PRIVACY-AWARE AMS MODELS

Sections 4 discussed privacy threats and threat actors that are relevant to the AMS scenario. In essence, the privacy literature that pertains the AMS scenario focuses on protecting user privacy – leaving the utility as the threat actor. The literature therefore proposes privacy measures with regard to preserving user privacy.

The majority of privacy-preserving schemes for the AMS scenario relate to privacy in the context of electric consumption measurements that address the following purposes and functions:

- Operational control
- Billing

Operational control. Operational control measures are not concerned with the consumption of individual users, but rather total loads on power lines and units in the network. Although there are control units at all levels in the power distribution grid, additional control is achievable by collecting fine-grained consumption measurements from users. As long as it is assured that individual measurements do not originate from specific identifiable users, but rather from a specific group of users, cf. anonymity sets (Pfitzmann, 2009), the privacy of the individual users is protected. User groups could, for instance, be established according the substation they are connected to.

Billing. In contrast to operational control, billing pertains to the consumption of individual users. Users must, at the time of billing, be linked to their consumption, which constitutes a loss of privacy for the users.

Attribution is the ability to identify the originator of a message that has been sent. Attribution pertains to whether measurements are linkable to specific smart meters or not, and relates therefore to linkability, which is a privacy threat as previously noted. In the privacy literature, unlinkability (non-attribution) is a common privacy goal. Measurements must be attributable for the utility to carry out billing, unless the billing is carried out at the user side, for instance by trusted devices such as trusted platform modules (TPM) or that verifiable means are used for user-side billing computation. On the other hand, attribution is not necessary for operational control purposes.

Operational control measures (load monitoring, load management) and variable-tariff billing require fine-grained measurements. Smart meters enable fine-grained measurement reporting, which pose a threat to user privacy in cases where measurements are attributable.

5.1 Privacy-preserving billing

In the AMS scenario, billing assumes fine-grained measurements. The overall privacy goal from the users' perspective is unlinkability, so that measurements cannot be linked to a specific user. This is in particular with regard to the utility, since the users do not necessarily trust the utility. This privacy requirement is contradictory with regard to the utility carrying out the billing function, since linkability is necessary for billing.

In the literature, essentially three approaches have been proposed:

1. Meter-side billing computation using trusted platform modules (TPM)
2. Meter-side billing computation using utility-side correctness verification by means of homomorphic cryptographic commitments
3. Utility-side billing computation by means of a trusted third party

The two first approaches suggest that billing computation is carried out at the smart meter, which hides measurements from the utility. Privacy is therefore assured, but requires that the billing computations are correct (i.e., assurance that the user did not cheat) and that the transmission of the billing amount is secure.

In the third approach, attributable measurements are disclosed, but sending them to an online TTP that does not reveal them to the utility, privacy is obtained with regard to the utility.

5.1.1 Trusted platform modules (TPM)

Petrlic et al. (2010) proposed to use trusted platform modules (TPM) integrated in smart meters for billing computation. No measurements are sent from the meter. The goal is to ensure the utility that the billing operations are correctly carried out, since the utility does not necessarily trust the users. This requires that price information must be securely transmitted from the utility and that the resulting amount information is securely transmitted from the TPM to the utility.

5.1.2 Commitments

Instead of sending measurements to the utility, the smart meter provides a proof (i.e., a commitment) to the utility for each measurement value, without revealing the actual measurement. At the end of the billing period, the meter computes and sends the billing amount to the utility. The already received commitments act as proof that the bill was computed correctly, providing assurance that the user did not cheat. Hence, the received billing amount is verifiable to the utility.

The idea is that for each measurement *m*, the smart meter sends a commitment *C* that is computed as a function of *C* and a secret random value *r*. Given a commitment *C* it is computationally hard to obtain *m* and *r*. At the time of billing, the smart meter computes and releases the dot-product *r'* of the random values and tariff vector. Due to homomorphicisms of commitment schemes, the utility uses *r'* conjunction with each commitment *C* and the tariff vector to verify that the billing price is correct. Commitment-based billing schemes are proposed in (Jawurek, 2011), (Rial, 2011) and (Borges, 2014).

5.1.3 TTP

Billing could alternatively be carried out by the assistance of a trusted third party (TTP). A straight-forward variant is that the smart meters authenticate and forward their consumption values to the TTP, which then computes the charging price that it forwards to the utility. Efthymiou et al. (2010) proposed using a TTP for both billing and operational control measures. Each smart meter is assigned two distinct long-term identifiers — one anonymous identifier (pseudonym) for fine-grained (high frequency) measurement reporting and one non-anonymous “regular” identifier for coarse-grained (low frequency) measurement reporting. Since the TTP that knows the mapping between these two identifiers, the TTP becomes a focal point of trust, with disadvantages such as vulnerability to insider threats.

5.2 Privacy-preserving operational control

The following approaches have been proposed for privacy-preserving operational control:

1. Privacy-preserving aggregation
2. Group signatures
3. Pseudonyms

The overall privacy goal is to give users assurance that their measurements are not made attributable to the utility. To obtain unlinkability, there must exist a number of possible meters that measurements can originate from, which is related to the terms anonymity sets and anonymity networks. As previously noted, another suggested approach is including an online trusted third party that both users and utility trust.

5.2.1 Privacy-preserving aggregation

Privacy-preserving aggregation for smart meters are secure-sum schemes that provide consumption aggregates from groups of smart meters. Aggregation schemes should be collusion-resistant to ensure privacy despite a number of colluding parties, including the utility.

Privacy-preserving aggregation schemes in general involve zero-sum blinding techniques. Measurements are blinded by means of randomness. When the blinded measurements from a group of smart meters are aggregated, the randomness is cancelled out, resulting in the sum of the measurements. The purpose of the blinding is to hide the individual measurement values, so that only the sum is realized. Most aggregation schemes have homomorphic properties, which is integral to the blinding.

We distinguish between two categories of privacy-preserving aggregation:

1) Interactive privacy-preserving aggregation.
2) Non-interactive privacy preserving aggregation.

We describe these categories next.

Interactive privacy-preserving aggregation

The majority of schemes in this category involve peer-to-peer message-exchange between all smart meters in a group.[1] More importantly, interactive scheme implies a high communication overhead that is the square of the number of meters and a computational overhead linear to the number of meters.
Schemes in this category usually work along the lines as follows:

a. Each meter randomly splits each measurement value into a number of partial shares. Comment: The (unpredictable) randomness causes the blinding.
b. Each meter sends one blinded share to each other meter, which then adds the received shares. Comment: Since a meter receives a blinded share from the other meters, confidentiality is achieved. The downside is the high amount of interaction.
c. Each partial sum is then transmitted to a central aggregator (the utility) that adds the partial sums. Comment: The utility has no way to deduce original measurements, and confidentiality is thus achieved.

This infers a round where each meter sends and then aggregates received partial shares and a second round where the aggregated partial shares are sent to the central utility. For *n* smart meters, the interaction overhead is therefore n^2 messages.

Regarding confidentiality, encryption may strictly speaking not be necessary due to that this is achieved by means of the blinding. Many, if not most, schemes use Pailler public key encryption, which have additive homomorphic properties. However, public key encryption does not provide message authentication.

[1] The scheme in (Busom, 2015) has in contrast bidirectional message exchange between each smart meter and the utility, which therefore makes this an interactive scheme as well.

Interactive privacy-preserving aggregation schemes commonly does not require a TTP.

The scheme proposed by Garcia et al. (2011) uses additive homomorphic encryption, for instance the Pailler cryptosystem. Each meter M_i encrypts the random partial shares with the public key of the other meters M_j , i <> j, respectively, and sends the *n* ciphertexts to the utility. The utility multiplies ciphertexts pertaining to each public key respectively, and sends the results back to the pertaining meters that each decrypts its received multiplied ciphertexts. Due to the homomorphic properties of the employed cryptosystem, the decryption restores the corresponding partial sums. These are sent to back to the utility that aggregates them. interaction overhead is therefore $n^2 + 2n$. The scheme provides user privacy if at least two meters are not corrupted.

(Klenze, 2014) is similar to (Garcia, 2011), but includes the user in such way that the user can contribute by randomness and check the execution of the protocol. A comment is that due to that measurements are reported periodically, it is therefore impractical to involve users.

The scheme proposed by Erkin et al. (2012) uses homomorphic encryption such as the Pailler scheme. There is no central utility. Instead of sending blinded partial measurements, each meter generates a random blinding value for each meter that it sends encrypted to the respective meters. Each meter aggregates the n-1 values it sent and the n-1 received random values, and encrypts the measurement and the aggregate random values w.r.t. each other meter and sends these ciphertexts to the other meters. At reception, each meter multiplies and decrypts, and obtains the aggregated measurement due to the homomorphicism. A “temporal consumption” scheme is also presented for privacy-preserving billing computation.

Dimitriou et al. (2016) proposed two schemes. The authors claim that the second scheme seeks “robustness” to account for when messages are dropped during execution of the protocol and modified. This is claimed to be achieved by means of a zero-knowledge mechanism. The second scheme is similar to (Erkin, 2012) and uses the Pailler cryptosystem. Instead of sending blinded partial measurements, each meter generates a random blinding value for each meter that it sends encrypted to the respective meters. Each meter aggregates its own random values and the received random values to the measurements, and sends the result encrypted to the utility that finally aggregates them. It is not clear if the robustness goal actually holds, because the meters have no way to be sure if sent messages actually are received. The overall problem is the lack of authentication mechanism, which would contribute to solve the mentioned problem.

Busom et al. (2016) presented a scheme that is based on the ElGamal public key cryptosystem. Each smart meter has its own public key that it uses to encrypt measurements that it additively blinds by a random integer. The utility multiplies (“aggregates”) one of the ElGamal ciphertext integers, and sends the product to each meter, which applies its private key and blinding integer to compute a decryption share that it sends back to the utility. Combining the decryption shares, the utility restores the aggregated consumption.

A point is that such schemes generally do not provide message authentication or entity authentication, which makes them susceptible to attacks such as replay attacks. Adding security measures such as message authentication codes (MAC) establishes message authentication.

Non-interactive privacy-preserving aggregation

Non-interactive schemes assume unidirectional communication from individual smart meters to the utility, which results in both low communication and computational overhead. In

principle, only one message needs to be sent from each meter. Group management of schemes that belong to category is predominantly static. This means that when a new meter joins a group or a meter leaves a group, then new keys must be securely generated and distributed to all pertaining meters and the aggregator. This implies the necessity of a trusted key center, which represents a single point of trust. From a privacy perspective, introducing a centralized single point of trust is in principle not desirable, because if this center is compromised, then all participants can be easily compromised too. Another point is potential vulnerabilities of insider threats.

The schemes presented by Shi et al. (2013) and Joye et al. (2014) require an offline trusted key center that is responsible for generating long-term keys. Given the long-term keys of a group of *n* smart meters, the key center computes an aggregated key that it securely assigns to the utility. Since the utility holds an aggregated key, individual meter keys are unknown to the utility. The most important disadvantage is that events of joining and leaving meters require a full key/share redistribution for all meters.

The scheme in (Leontiadis, 2014) is based on (Shi, 2013) and (Joye, 2014) and requires no key dealer, and therefore avoids a key center, representing a single point of trust. Each meter key is generated independently. However, for practical smart metering systems it can be argued that this is not a real issue, since smart meter manufacturers supply encryption keys into the smart meters at production. The mentioned scheme introduces an online semi-trusted entity, the 'collector', whose function is to aggregate so-called auxiliary shares provided by each meter. The downside is that if the collector and aggregators collude, then individual measurement values can be obtained, and privacy is breached.

A variation of the mentioned schemes are presented in (Benhamouda, 2016), which uses so-called smooth projective hashing.

All the mentioned non-interactive schemes employ timestamps and have therefore non-reusability/freshness assurance.

5.2.2 Group signatures

Group signatures provide a proof that the signer is associated with a group, but does not reveal the identity of the actual signer. However, group signature schemes have a feature that allows a group manager to reveal the original signer. For the purpose of operational control measures, group signatures provide unlinkability for smart meters that continually transmit fine-grained measurements to a utility. For examples, see (Zargar, 2013) and (Kishimoto, 2017).

Group signatures can also be used for billing, but then the utility's billing center has the authority to reveal signers (Chan, 2014), in which case the billing center has the equivalent role of a trusted third party and becomes a focal point of trust, which is not desirable. Another downside is that group signatures are computational intensive.

5.2.3 Pseudonyms

Some authors propose using pseudonyms as a means for anonymization and privacy (Afrin, 2016). In order for a pseudonym to be trustable, it must be verifiable. This could be realized by means of anonymous certificates, which requires an issuing trusted third party. Schemes using anonymous certificates are found in (Efthymiou, 2010) and (Petrlic, 2010). The downside is the trusted third party. Disclosure of the secret pseduonym/meter-relationship compromises the privacy. Another point is that certificate-based pseudonyms are static, which limits the efficacy of the unlinkability. Finally, certificates require asymmetric

cryptography, which is considerably more computational intensive than symmetric cryptography.

5.3 Combined: Operation & billing

Borges et al. (2014) presented an aggregation scheme for operation monitoring that includes billing verification. It uses Pailler encryption and Pedersen commitments. The billing charge is computed at the meter side, so tariff data need to be transmitted to the meters. The commitments are used by the utility to verify the correctness of the meter-side billing computation.

Other combined privacy-preserving schemes for billing and operation are found in (Rial, 2011) and (Efthymious, 2010).

5.4 Literature surveys

Erkin et al. (2013) present an overview of four aggregation schemes for smart meters, whereof three are presented in this report.

A survey of privacy-preserving schemes for the two noted areas of billing and operation is provided in (Asghar, 2017). Table 3 shows a list and comparison of papers with regard to the chosen method of a paper and supposed privacy and security properties. The claimed properties may not be actual for some of the papers.

Ferrag et al. (2016) provide an overview according to the categories 1) Smart grid with the advanced metering infrastructure, 2) Data aggregation communications, 3) Smart grid marketing architecture, 4) Smart community of home gateways, and 5) Vehicle-to grid architecture.

5.5 Predictive analysis on encrypted smart meter measurements

Statistical predictive analysis may be desirable to carry out. In (Habtemariam, 2016), the authors present the case where the utility has outsourced the task of statistical predictive analytics to a separate untrusted third party (the cloud?), which accordingly must be prevented from reading actual measurements. Hence, user privacy is to be preserved with regard to the untrusted third party, not the utility. The authors propose regression computations to be carried out on measurements that are encrypted using the homomorphic Pailler encryption algorithm. Regression results remain encrypted, and are sent back to the utility that decrypts them.

5.6 Recommended directions

The mentioned privacy-preservation methods are based on the assumption of anonymity sets, which assumes that smart meters in operation belong to a group. Physical proximity is a natural decision factor to determine group membership. We consider the ability of dynamic group membership (new smart meters added to a group and existing meters leaving the group) as to be a relevant requirement. It should also be convenient to establish and add meters to a new group.

Group signatures and pseudonyms are suitable for operation monitoring, but not billing verification, since this operation requires the link between a user identity and the user's consumption, where the latter may be represented as a verifiable dot product of the measurement and tariff vectors. Group signatures are computational intensive and do not conform to dynamic group memberships. Pseudonyms are mainly used for anonymization, which is not the primary privacy goal here: They also rely strongly on a trusted third party and/or digital certificates, where the latter have the downside of being computational intensive.

For privacy-preservation of smart meters we suggest non-interactive aggregation, since this avoids the disadvantages of the high smart meter communication interaction and encryption overhead that pertain to interactive schemes. For this task, we will propose and implement a non-interactive privacy-preserving aggregation scheme that supports dynamic group management, which will avoid the disadvantages of having full key redistribution of joining and leaving meters. If time allows it, privacy-preserving billing will be considered.

6 CONCLUSIONS

In this report, we present an overview of privacy-aware models and related measures of privacy or smart meters. A presentation of privacy concepts such as privacy threat actors and privacy threats, that is applicable to smart meters, is also provided. We suggest non-interactive privacy-preserving aggregation, considering its comparatively low message and computational overhead. Dynamic group management support avoids the disadvantages of full key redistribution of joining and leaving meters, and is highly desirable regarding practicality. This feature will therefore be investigated for this task. Privacy-preserving billing will be considered if time allows

7 REFERENCES

Marit Hansen (2012). Top 10 mistakes in system design from a privacy perspective and privacy protection goals. In: Privacy and Identity Management for Life. IFIP AICT 375. Springer, p.14–31.

Andreas Pfitzmann and Marit Hansen (2009). A terminology for talking about privacy by data minimization: Anonymity, Unnlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management (v0.32).

Mina Deng, Kim Wuyts, Riccardo Scandariato, Bart Preneel, and Wouter Joosen (2011). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requir. Eng. 16, 1 (March 2011), 3-32.

Costas Efthymiou and Georgios Kalogridis (2010). Smart grid privacy via anonymization of smart metering data. In 2010 First IEEE International Conference on Smart Grid Communications, pages 238 – 243, 11.

F. Borges, D. Demirel, L. Böck, J. Buchmann, and M. Mühlhäuser (2014). A privacy-enhancing protocol that provides in-network data aggregation and verifiable smart meter billing. In 2014 IEEE Symposium on Computers and Communications (ISCC), pages 1–6, June 2014.

Ronald Petrlic (2010). A privacy-preserving concept for smart grids. In Sicherheit in vernetzten Systemen: 18. DFN Workshop, pages B1–B14. Books on Demand GmbH, 2010.

Marek Jawurek, Martin Johns, and Florian Kerschbaum (2011). Plug-in privacy for smart metering billing. In Proceedings of the 11th International Conference on Privacy Enhancing Technologies, PETS'11, pages 192–210, Berlin, Heidelberg, 2011. Springer-Verlag.

Alfredo Rial and George Danezis (2011). Privacy-preserving smart metering. In Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society, WPES '11, pages 49–60, New York, NY, USA, 2011. ACM.

Flavio Garcia and Bart Jacobs (2011). Privacy-Friendly Energy-Metering via Homomorphic Encryption, pages 226–238. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

Tobias Klenze (2014). Privacy strategies in smart metering. 2014.

Tassos Dimitriou and Mohamad Khattar Awad (2016). Secure and scalable aggregation in the smart grid resilient against malicious entities. Ad Hoc Netw., 50 (C):58–67, November 2016.

Zekeriya Erkin and Gene Tsudik (2012). Private Computation of Spatial and Temporal Power Consumption with Smart Meters, pages 561–577. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

Iraklis Leontiadis, Kaoutar Elkhiyaoui, and Refik Molva (2014). Private and Dynamic Time-Series Data Aggregation with Trust Relaxation, pages 305–320. Springer International Publishing, Cham, 2014.

S.H.M. Zargar and M.H. Yaghmaee (2013). Privacy preserving via group signature in smart grid. In Proceedings of the Electric Industry Automation Congress (EIAC), February 2013.

H. Kishimoto, N. Yanai, and S. Okamura (2017). An anonymous authentication protocol for smart grid. In 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), pages 62–67, March 2017.

D. He, S. Chan, Y. Zhang, M. Guizani, C. Chen, and J. Bu (2014). An enhanced public key infrastructure to secure smart grid wireless communication networks. IEEE Network, 28(1):10–16, January 2014.

Torben P. Pedersen (1992). Non-interactive and information-theoretic secure verifiable secret sharing. In Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '91, pages 129–140, London, UK, 1992. Springer-Verlag.

Elaine Shi, T.-H. Hubert Chan, Eleanor G. Rieffel, Richard Chong, and Dawn Song (2011). Privacy-preserving aggregation of time-series data. In Network and Distributed System Security Symposium (NDSS 2011). The Internet Society, 2011.

Marc Joye and Benoît Libert (2013). A Scalable Scheme for Privacy-Preserving Aggregation of Time-Series Data, pages 111–125. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

Fabrice Benhamouda, Marc Joye, and Benoît Libert. A New Framework for Privacy-Preserving Aggregation of Time-Series Data. ACM Trans. Inf. Syst. Secur. 18, 3, Article 10. 2016.

Nuria Busom, Ronald Petrlic, Francesc Sebe, Christoph Sorge, Magda Valls. (2016). Efficient smart metering based on homomorphic encryption, In Computer Communications, volume 82, pp. 95–101, 2016.

Zekeriya Erkin, Juan Ramón Troncoso-Pastoriza, R. L. Lagendijk, Fernando Pérez-González (2013). Privacy-Preserving Data Aggregation in Smart Metering Systems: An Overview. IEEE Signal Processing Magazine. 30. 75-86. 10.1109/MSP.2012.2228343.

M. R. Asghar, G. Dán, D. Miorandi and I. Chlamtac (2017). Smart Meter Data Privacy: A Survey. In IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2820-2835, Fourthquarter, 2017.

Mohamed Amine Ferrag, Leandros Maglaras, Helge Janicke and Jianmin Jiang. (2016). A Survey on Privacy-preserving Schemes for Smart Grid Communications.

B. Habtemariam, A. Miranskyy, A. Miri, S. Samet and M. Davison (2016). Privacy Preserving Predictive Analytics with Smart Meters. IEEE International Congress on Big Data (BigData Congress), San Francisco, CA, 2016, pp. 190-197.