FROM A BARRIER TO A BRIDGE: DATA-PRIVACY IN DEREGULATED SMART GRIDS

Completed Research Paper

Jens Strüker
University of Freiburg
Friedrichstr. 50
79098 Freiburg, Germany
strueker@iig.uni-freiburg.de

Florian Kerschbaum
SAP Research
Vincenz-Prießnitz-Str. 1, 76131
Karlsruhe, Germany
florian.kerschbaum@sap.com

Abstract

The introduction of so-called smart meters involves detailed consumption data. While this data plays a key role in integrating volatile renewable energy sources, a side effect is that it can reveal sensitive personal information. Concerns and protests led to a stopped smart meter rollout yet. In deregulated electricity markets, data-privacy is even more at risk: The UK, Texas and Ontario decided for a nation-wide communication intermediary in order to facilitate the exchange of the vast amount of smart meter data. However, this operational efficiency is achieved by the fact that an intermediary is a single point of failure. We present an approach based on encryption to secure the intermediary against privacy invasions and we can show that our prototypical implementation meets even restrictive requirements for large-scale data handling and processing. By aiming at customers' confidence in smart metering, our solution might lay the ground for an ecosystem of energy services.

Keywords: Data privacy, Data security, Digital business ecosystems, Information systems security and privacy

Introduction

The global climate challenge of decarbonizing today's electricity system is inseparably linked to a smarter grid. While the integration of a growing share of renewable electricity sources such as sun and wind means less fossil fuel power plants, this substitution of a few baseload and central plants with a plethora of intermittent and distributed electricity generation will increasingly lead to coordination challenges within the electricity system. Accordingly, reading a mechanical residential or commercial electricity meter once a month and planning the electricity supply based on so-called standard load profiles is not in keeping with the times. The digitization of the electricity system, i.e. adding an additional communication layer on top of the electricity grid, is therefore seen as a necessary step to decarbonize our electricity systems.

The foundation of such smart grids is a two-way communication network interconnecting many components so that utilities and customers can exchange information in an interactive real-time manner. The Advanced Metering Infrastructure (AMI) as part of this communication system provides accurate readings automatically at requested time intervals (e.g. DECC, 2010). Legislators all over the world intend to motivate consumers to save energy by providing them more frequently with more detailed consumption information. Based on this information and the possibility to send price signals back to the customers within short intervals, utilities are also able to shift demand from peak to off-peak times by using time-of-use, critical-peak or real-time prices. Experts agree on the necessity of this kind of demand side management in order to integrate an increasing share of intermittent and also distributed renewable energy sources such as wind and solar in the power system. Because information is ultimately what makes the grid intelligent, smart metering could prove to be the equivalent of bar coding for supermarkets - automating the data-gathering process changed the retail industry forever. However, the fine granularity power consumption data has raised privacy concerns and has been widely discussed in the media (e.g. Barringer, 2011) and reports by data protection authorities (e.g. NIST, 2010; Task Force Smart Grids, 2011).

User data privacy comes into play as smart meter data can reveal sensitive private information about electricity users. Research shows that personal information such as an individual's habits, behaviors, activities, preferences, and even beliefs can be estimated with high accuracy by using so-called nonintrusive appliance load monitors (NALM) (e.g. Rajagopalan et al, 2011). By analyzing energy signatures to track appliance usage patterns (Lam et al., 2007) (Quinn, 2009), these monitors provide means to identify appliance usage even when multiple household power signatures are aggregated (Laughman et al., 2003). The privacy concern is that this energy use information can be repurposed by interested parties (Cho et al., 2010; McDaniel and McLaughlin, 2009). Kologridis et al. (2010) argue that this privacy threat goes beyond the exposition of private to a common 'spy' because AMI would facilitate the analysis of this data on an industrial scale. While credit card companies certainly know a consumer's spending profile and Google knows what individuals are doing at a very granular level, there is a decisive difference: One can always choose not to use Google, or a particular credit card. NIST pointed out in 2011 that the major benefit provided by a smart grid, i.e. the ability to get richer data to and from customer meters and other electric devices, is also its Achilles' heel from a privacy viewpoint (NIST, Fang et al., 2011).

Consequently, if both the incentive for opportunistic behavior and the possible damage are so huge, *security policies and legislation* may not be sufficient to guarantee user data privacy or to build trust of customers in future smart grids. This opens up possibilities for *technological-based protection solutions*. However, Rajagopalan et al. (2011) argue that the consequences of the smart grid privacy problem are hard to understand yet because the full range of information extraction possibilities is not known. Additional uncertainty is created as so many different smart grid communication architectures are discussed right now. As a consequence of the EU Directive 2006/32 and the EU 20-20-20 climate goals, for example, all EU member states are going to implement a smart metering infrastructure in the coming years. In the US, the situation is similar in many states and while 75 percent of the electric meters in the U.S. are expected to be digital meters by 2016 (Fehrenbach, 2012), the realized and planned communication architectures are anything but homogeneous.

In the scope of a stopped smart meter roll-out in the Netherlands in 2009, it was discussed that a thief could use the data to see when homeowners were around and plan break-ins. Another concern was that governments could spy on citizens, as could insurance companies to set rates. While all these cases require

an unauthorized disclosure of smart meter data, there is a more obvious but not less problematic threat. Fine-granularity power consumption data provides a utility with a great deal of commercially valuable information about how and when consumers use their energy. That opens the relationship between the utilities and their clients to potential abuse. Fan et al. (2012) remind us that if there is a clear financial incentive, legitimate techniques for mining and exploiting data will quickly evolve. This is, at least, what we could learn from the past. Accordingly, technological-based solutions could be of great help if they were able to reduce both the risk of unauthorized disclosure and abuse of smart meter data. Those approaches could, for instance, allow utility providers to use only the data in an acceptable manner or detect (in retrospect) misuse of smart metering data. Even a sound *documentation* of events through logging and audit mechanisms could be discouraging for misuse and prove to be a reasonable complement to existing security policies and legislation.

In this contribution, we first identify the different market actors with their interest in smart meter data in *deregulated* electricity markets and show how the numerous interests and interactions complicate the data privacy challenge by several orders of magnitude. As a result, we argue that deregulated electricity markets, such as in the entire EU, Texas, Ontario and many more, require some form of intermediaries to reduce this complexity. Subsequently, we describe our research design and derive requirements to a data exchange intermediary. We then review existing privacy-enhancing technologies for smart grids and finally present our specific solution for maintaining user data privacy in deregulated smart grids with an intermediary.

Need for Data Exchange Intermediaries

The Complex Relationships in Deregulated Electricity Markets

The communication requirements in a deregulated electricity market differ significantly from those in a regulated market. As Strüker et al. (2011) illustrate, the challenge in a *regulated* market, where one integrated monopolistic utility is responsible for electricity generation, distribution and sale, is confined to the technical communication between smart meters and the utility and the subsequent processing of the meter data with enterprise applications. However, things get more complicated in a *deregulated* market such as in the European Union. While there is still one electricity distribution grid operator responsible for any given geographical area, customers can choose from many suppliers and in some member states even from several meter operators. Meter operation can be carried out either independently or performed by suppliers or distributors, as national regulations require. Moreover, people can switch their electricity supplier – in the UK, 17% of electricity customers switched their supplier during 2010 at least once (Ofgem, 2011).

In future *deregulated smart grids* with a large share of intermittent renewables (>20%), measurement data is needed in different forms for different purposes by the different market actors (e.g. Pallas, 2012). Accordingly, the distribution grid operator requires detailed consumption data in short time intervals, smart meter device address, power quality data such as voltage data, outage data and date and time stamps in order to balance and stabilize the grid (Strüker et al, 2011). Electricity retailers need detailed consumption data for dynamic tariffs, such as time-of-use and critical peak pricing, and data in short term intervals for real-time pricing. Furthermore, billing and relocations of residential customers also require detailed consumption and so-called point of delivery (POD) data (market communication). In this context, Strueker et al. point out that the data exchange between retailers and smart meter operators or distribution grid operators is complicated by retailers serving many geographies and endpoints, i.e. they can have customers in different distribution networks. This creates a substantial combinatorial problem of who should access what information. According to (BDEW, 2012), German household customers, for instance, can choose on average among 102 electricity suppliers. In total, there are roughly 1,100 electricity suppliers and more than 800 distribution networks in Germany. If third parties - such as demand respond aggregators, energy management providers or providers of new value-added services such as care of the elderly –also get access to residential energy consumption data (cp. California[1]), this will lead to even more dynamic and volatile business relationships among the market actors and,

[1] The California Public Utilities Commission has adopted a policy that utilities must give access to energy consumption data to individual consumers and their appointed third-party providers by the end of 2010 and then provide the data in a somewhat real-time manner by the end of 2011.

accordingly, coordinating the exchange of data between smart meters and the various market participants entitled to this data will be complex. A data exchange intermediary is seen as an option to reduce this complexity.

Data Exchange Intermediaries in Emerging Smart Grids

There are at least three options to organize the smart meter data exchange in deregulated markets: States can (i) monopolize and regulate the nationwide data exchange, (ii) prescribe the data exchange as an additional and regulated task of the distribution network operators or (iii) do not interfere in the exchange at all. Due to the described complex communication challenges, Ontario, Texas and the UK decided for a single regulated and monopolized data exchange intermediary for their liberalized market regimes, i.e. option (i). Their intermediary in the electricity market is an information system distributing messages, i.e. sending messages from smart meters to enterprise systems and vice versa and also between applications across enterprises. An intermediary reduces the complexity significantly due to its sheer existence*:* When a network consists of S + A participants, only S + A relationships have to be managed. However, without a central organization, i.e. an intermediary, S x A relationships have to be dynamically managed in the entire network. From the cost side, intermediaries are therefore a promising solution to the data exchange challenge in smart grids. If the data exchange is a task of the distribution grid operator – i.e. option (ii) – and there are many of them (>800 in Germany), the complexity would be still high. Against the background of security of supply (critical infrastructure) and the importance of the data exchange both for market communication and managing the future smart grid, governments are unlikely to wait and see whether the market will create intermediaries without too much market power or capable intermediaries at all. Option (iii) could therefore prove to be merely a theoretical choice.

Before we show what privacy and security implications such an intermediary has and what privacy protection mechanisms have been proposed, we first look at the broad spectrum of different roles and responsibilities such an intermediary can take on (s. Table 1). Similar to systems in Ontario and in Texas, the UK government decided that the smart meter rollout should include a *centralized* meter data communications provider and data exchange (DECC, 2010). As illustrated in Table 1, this central entity is going to operate the communication network for AMI data, run a data repository, perform basic translation services, but will do no data processing such as billing or analysis. Consequently, this intermediary can be described as a data hub.[2] In Texas, five regulated transmission and distribution service providers collect the smart meter data and send it to a web portal.[3] This web portal provides consumption data while the processing is done by the retail electricity providers who get access to the data. Unlike the British and the Texan intermediary, the Meter Data Management/ Repository (MDM/R) in Ontario receives meter readings from all AMI in Ontario, and then processes the readings to produce billing quantity data to support billing, stores and manages data, and provides access to licensed retailers.[4]

Regarding the data exchange intermediary, the designer can choose between a storage facility and an event-based distribution facility. Storage facilities have the clear advantage of data consistency among participants. Every actor accesses the same data that can also be efficiently updated. Also consistent meta-data, such as security policies can be applied to all data and efficiently updated. Furthermore, storage facilities reduce the overall costs, since – as a whole – less storage capacity is necessary than in a decentralized approach. In terms of reliability both approaches represent a single point of failure and need to implement appropriate countermeasures. Clearly, the advantages of a storage facility are compelling.

[2] Please note that this scenario follows the British regulator's 'current scope' and that the discussion will continue until the end of 2013.

[3] See www.SmartMeterTexas.com.

[4] See www.smi-ieso.ca/mdmr.

	Texas	Ontario	UK
Market regime	Regulated transmission and distribution service providers (5 TDSP's)	Competitive wholesale market and centrally procured or regulated supply	Competitive wholesale and generation market; domestic customers switch often.
Exchange infrastructure	Smart Meter Texas Web Portal 6 million installed smart meters	Meter Data Management/ Repository (MDM/R), run by the Independent System Operator (IESO), 8 million installed smart meters	DCC, Data Communications Comm, centralized data repository. 54 million installed smart meters by 2019
Time interval of data *collection*	15-minute interval	Hourly	Half an hour
Time interval of data *transfer*	Every four hours	Monthly	Half an hour
Information flow	TDSP collect data and communicates to the web portal; instant access to meter data by customer and retail electric providers	Data is directly collected through the Local Distribution Companies (LDC) and then transferred to the (MDM/R)	DataCommsCom (DCC) will receive the data and then provide the data to authorized parties
Interaction with smart meters	Only read events yet (one-way communication); Retailers shall use TDSP networks to send home area network (HAN) commands via ZigBee SEP 1.0 interface	Read events (one-way communication)	Smart meters with two-way-communication capabilities
3rd parties access to smart meter data	Only licensed retailers, third parties are in discussion	Only licensed retailers, third parties are in discussion	Third parties will get access to customer consumption data
Functionalities and added-value services	Portal only provides data, processing done by retailers; storage of consumption data, Home Area Network registration; Planed: enhanced security, data reporting, exporting and on demand reads	Meter reads and reports, data transmitted for billing, requests for data; storage and processing of data submitted by nearly 80 Local Distribution Companies (LDC`s)	Initially limited to effective transfer of data new functionalities after deployment in discussion
Data privacy and security	Only customers own smart meter data (Texas Utilities Code 39.107(b)); VPN tunneling; access control mechanisms and logging and monitoring of all system and application components (http://goo.gl/J0qIu)	Internal access control systems to protect smart meter data (http://goo.gl/sFuXY).	Under discussion (http://goo.gl/1VJoe)

Table 1: Data Exchange Intermediaries in Deregulated Markets

Research Design

It is conceivable that intermediaries will take on different roles in different countries. Besides the choice between pure data hubs and added value service providers, states can also decide for more than one intermediary which additionally can be regulated or not (cp. Strüker et al, 2011). In Germany, for instance, there will be no nationwide central intermediary storing smart meter data due to constitutional concerns (Federal Network Agency, 2011). Intermediaries acting as a 'post office' by distributing messages between the smart meters and different market actors and storing smart data for a while are a realistic option for all the states that will build up a data exchange infrastructure in the coming years. Our research tackles the problem of how to secure data exchange intermediaries in future smart grids. We address this problem by using the well-known design science research approach (e.g. Hevner et al. 2004) to develop an IT artifact that enables residential, industrial and commercial customers to exchange data with other market actors in a smart grid in a confidential manner.

The design science methodology seeks to create IT artifacts that are intended to solve specific organizational problems and provide rigorous evaluation of these artifacts based on utility rather than an empirical test of theories. This encompasses successive steps of problem identification, definition of objectives for a solution, design or development of a suitable IT artifact, and demonstration of the proof of concept, evaluation, and communication (Hevner et al. 2004). Accordingly, we first identify the basic assumptions and boundary conditions of the data exchange in smart grids and then derive generalizable requirements of an abstract privacy-preserving system. Clearly, the amount of regulation underpins that privacy in the smart grid represents a relevant business problem (principle 2). We discuss proposed solutions to the privacy problem by screening the privacy-enhancing technology literature and subsequently present our mechanism to secure the smart grid intermediary. We derive functional and security objectives for our method of encrypting the smart meter data. We therefore used rigorous methods in our design (principle 5). We emphasize that the intermediary will only handle encrypted data, such that we elaborate our key distribution and revocation scheme meeting these objectives and circumventing the common drawbacks of encryption-enforced access control. This approach is the result of well-educated search process on available technologies (principle 6). We then develop the

corresponding method with an instantiation and, subsequently, evaluate its performance characteristics. For security, we rely on the rigorous security proofs of the encryption method. Our scheme is secure if the underlying encryption scheme is secure. We use measurement of a prototypical implementation using statistically sound result reporting. We therefore use rigorous methods to evaluate our design (principle 3). We anticipate making a substantial contribution to the field by our results, but also by outlining the problem and identifying directions for future research (principle 4). The participation of industrial co-authors ensures the dissemination in industry (principle 7).

Requirements to a Data Exchange Intermediary

The public debate preceded the intermediaries' introduction in Ontario, Texas and the ongoing discussion in UK, the Netherlands and Germany revealed a couple of trade-offs between IT-security and data privacy, market efficiency, innovation and the stability of the Grid (Rajagopalan et al., 2011; DECC, 2010; DECC, 2011; Raven, 2010). There is, for instance, recognition that following the data minimization principle and therefore restrict third party access to detailed customer consumption data can stifle innovation and restrict benefits to electricity consumers (e.g. DECC, 2011). A literature review shows that these conflicts were not yet incorporated in pertinent information systems or energy journals (Strüker and v. Dinther, 2012). We next want to identify the relevant data privacy conflicts and determine requirements to a data exchange intermediary in future smart grids with a high share of renewables. Consequently, we focus on the trade-offs between data privacy on the one hand and market efficiency, innovation and stability of the grid/ security of supply on the other.

In deregulated smart grids with a large share of renewables, the supply side becomes very volatile. Because investing in additional back-up generation, grid-scale storage facilities and new transmission lines are expensive and take time to develop, demand-side managing via price signals or other incentives is seen as a promising solution to increase market efficiency. Besides interacting with power customers, detailed power consumption data is required in order to know how and when to incentivize whom. As more and more distributed power generations, such as wind turbine or solar panel, are installed on the distribution grid level, the power system becomes significantly more dynamical than the traditional one. Hence, the distribution grid operator will demand much more frequent reports, whose interval may be reduced to at most a few seconds or even less. The real-time requirement and the large number of power users and generators on the distribution grid level bring a significant challenge to the load management (Gong and Li, 2011; Ramchurn et al., 2012). If we assume that third parties will have access to smart meter data (cp. Table 1) or can interact with smart meters in order to build novel data-based energy services on top (cp. ecofactor.com or opower or demand response providers such as entelios.com), additional demand for consumption data at (near) real-time resolution will be created (Ramchurn et al., 2012, Strüker et al., 2011). In summary, market efficiency, innovation and grid management will require detailed consumption data.

In the introduction, we showed that gathering detailed smart meter data is a considerable potential privacy threat. At the same time, this data is needed for maintaining the security of supply, innovations and market efficiency. Thus, the question arises of how the traditional energy companies (smart meter operator, grid operator, retailer etc.) can protect their customers' data privacy, while at the same time letting service providers from outside the electricity industry access that data? How can one give the customers control over their data and make the electricity system future-proof at the same time? In the following section, we will review privacy-preserving mechanisms and check whether they are an appropriate solution to the challenges in a *deregulated* smart grid with one or a couple of communication intermediaries.

Privacy-preserving Mechanisms for Deregulated Smart Grids

Privacy in the deregulated smart grid is an instance of the well-known problem of privacy in the Internet of Things. A number of trustworthy sensors collect personal information that must be processed in a privacy-preserving manner. As such many approaches investigated in this context, e.g. for the credit card industry, may potentially be adapted to suit privacy in the smart grid. Nevertheless there are also a number of differences that make the privacy problem in the smart grid more complex than previous cases. First, smart meters are commonly required by law and are not an optional contract consumers may arrange. Therefore privacy also needs to be mandatorily protected. In the credit card industry we see little

privacy protection which is clearly not acceptable for a regulated scenario. Second, in the deregulated smart grid there are a number of participants that all need to use the data and for very different purposes using different algorithms. The same data is used by different market participants for obligatory purposes such as network management, billing, and demand response, but also optional purposes such as advertising and many more. Therefore a single cryptographic solution, such as privacy-preserving electronic payments in the credit card industry, is not applicable. We address this by providing a generic, but privacy-preserving data exchange platform that suits even applications not yet developed.

A number of technological solutions have been proposed in order to maintain data privacy in smart grids. Fan et al. (2012) give a rough overview of different approaches and lists some respective research contributions (Efthymiou and Kalogridis, 2010; Costas and Kalogridis, 2010; Rajagopalan et al., 2011; Bohli et al., 2010; Garcia and Jacobs, 2010; Kim et al., 2011). While research on privacy in smart grids from an Information Systems angle is still in its infancy (cp. Wicker and Thomas, 2011; Strüker and van Dinther, 2012), computer scientists and engineers researched extensively on privacy-enhancing technologies for smart grids (Rajagopalan et al., 2011; Fan et al., 2012).

In order to address the privacy issues of smart meter data and communication in smart grids in general, **anonymization** techniques shall prevent the assignment of consumption data to individual persons. However, a couple of researchers (e.g. Gong, 2011; Pallas, 2012) and many practitioners (cp. public debate in UK: DECC, 2012) have pointed out that processes such as accurate and high resolution billing in an energy system with a significant share of distributed renewable energy sources and many market actors require personal or at least personalizable data. Novel energy management and demand side management services demand power consumption information at a level of granularity far finer than that needed for monthly billing (Walawalkar et al., 2010). Moreover, these services have to interact with energy customers, i.e. they have to link consumption data to individual customers. Furthermore, Jawurek et al. (2011) successfully performed a number of re-identification attacks on anonymized smart meter data, such that the effectiveness of anonymization for the protection of privacy is already in question.

Data minimization is a well-known principle of data protection and refers to the restriction of data collection, processing and use to the smallest possible amount. The idea is that only data that proves absolutely essential shall be communicated to external parties. Privacy-enhancing technologies are designed for internet-based communication and many of them are based on data minimization (e.g. Clauss et al., 2002). Consequently, data minimization also found its way into the smart grid data privacy research (e.g. Yan et al., 2011). Beyond academia, this principle plays a major role in the context of smart metering introductions as well (BSI, 2011b). In Germany, for instance, the Federal Office for Information Security has developed a protection profile for smart meters (gateways) that prescribes data minimization as a core principle for smart meter communication (BSI, 2011a). It is unquestionable that restricting data uses from the outset is an effective means to protect the customer from his/her data being misappropriated. However, this inevitably requires a complete ex-ante definition of legitimate data uses (Pallas, 2012). This is a contradiction to a dynamic liberalized electricity market with third party access to customer data and ever-changing relationships (e.g. switching suppliers). In addition, without interaction (e.g. sending a price update to the meter) and detailed meter readings, additional services are impossible, such as time-based tariffs (detailed time of use tariffs), variable price contracts (real-time pricing) and demand side management. All these shortcomings also hold true for the **aggregation** approach. Instead of anonymizing personally identifiable information, i.e. consumption data, the data is aggregated to a degree that eliminates any link to an individual consumer.

Subsidiarity is another principle that applies to privacy protection schemes for smart grids and is also related to data minimization (e.g. BSI, 2011b). When collected, data is to be used locally wherever possible. The underlying idea is that local system environments are controllable and therefore trustworthy. Accordingly, the goal is to empower consumers to manage much of the energy information inside the household without having to share personal consumption data with their energy suppliers. Storing at and pre-processing consumption with the smart meter is an example. As this overall offers a high level of data privacy, following this principle comes at high costs though. First, the customer now has to manage all the different relationships with today's data receivers (smart meter operator, distribution and transmission service operator, supplier etc.). Against the background of future development of innovative, not yet foreseeable data-intensive services, Microgrids and local electricity markets, this is likely to overburden consumers. Additionally, data-privacy is not the only factor affecting the utility function of a customer. In order to make a rational decision, customers need to know what the opportunity monetary costs of local

storage and processing are (Rajagopalan et al., 2011). Energy management services based on analyzing very big data volumes in the 'cloud', for instance, enable more options and more effective services than services based on local data only. Moreover, cloud-based applications promise to learn quickly by comparing consumption behaviors etc. and save cost by avoiding software-update and maintenance efforts. Storing consumption data in the home brings additional complexity to the move in/move out process (MIMO) and finally shows a significant privacy risk: When an occupier moves and does not want the new occupants to have access to his consumption data, the data mastered on meters will have to be deleted or passed on to the new residence (Ravens, 2010). These critical processes mean an additional burden for customers. Aside MIMO, this problematic is also relevant for customers switching their supplier (remember that 17% of electricity customers switched their supplier in the UK in 2010).

Encryption is a promising tool to guarantee a secure smart meter data communication. As data needs to be disseminated to many different stakeholders within the grid in liberalized and unbundled electricity markets, the use of access control mechanisms, e.g. secure authentication, authorization and confidentiality services, is, however, challenging. And in fact, although *federated* security management solutions have been proposed for a smart home environment (e.g. Khouri et al., 2009) and end-to-end encryption based on a public key infrastructure (i.e. for a chain of users) is said to be state of the art for many years[5], approaches where a smart meter serves as a *policy* or *authorization* engine in the complex and dynamic environment of a deregulated electricity market are not yet available. Once millions of smart meters and thousands of e-vehicles are to be integrated into an event-driven or service-oriented architecture within a liberalized market regime, the question of a federated encryption management ultimately will arise. Setting up and *automating* the required authorization and authentication processes in such a dynamic environment poses great challenges for the design of the smart grid communication system.

Fan et al. (2012) point out that future protection schemes are likely to be a combination or evolution of the principles illustrated above, depending on factors such as system cost or the need for privacy in different societies. As we have shown, we see the market regime as an additional and crucial factor. Jawurek et al. (2011b) and Rial and Danezis (2011) propose verifiable computations using zero-knowledge proofs for smart meter billing, but these solutions are limited to an end-to-end scenario and cannot take advantage of a data intermediary. Thus, we think that encrypting the smart meter data and the communication between the market actors and a smart meter has to be at the core of any sustainable and future-proof privacy-preserving solution. Nevertheless, if we weigh the potential of an intermediary to reduce complexity and its disadvantages (the single-point of failure argument in particular), an intermediary seems to be indispensable. Such a communication intermediary can also play a crucial role in the context of federated encryption management: A communication hub that stores high-resolution measurement data centrally for any given district might be able to balance the trade-off between privacy and performance. One of the decisive challenges therefore is to secure the storing of consumption data at the intermediary and to find a substitute for the fact that the customer is no longer in control of his/her data.

Securing the Data Exchange Intermediary

Storing smart meter data at an intermediary involves number of security and trust issues. **Security** is critical because the data repository at the intermediary represents a valuable target for hackers. A heightened investment in security is necessary. Not only hackers, but also insiders represent a notable threat. There already have been cases documented where administrators leaked data outside their company (Hildenbrand et al., 2011). **Trust** is critical because the intermediary controls the dissemination of the data. In the best case, the homeowner is able to **specify his/her access control rules**, but at least **enforcement** is entrusted to the intermediary. The **data owner is no longer in control**.

We intend to improve both aspects by encryption. The idea is to encrypt the data by the data owner and distribute the keys to authorized recipients. Neither a hacker nor an insider is then able to access the data at the intermediary, since it is encrypted. Furthermore, the homeowner controls access by his/her choice of encryption keys. Enforcing access control by encryption is a well-studied topic (e.g. Miklau and Suciu, 2003). Its main problems are

[5] Cp. the EU funded research project MUSE, Specification of a multi-service RDG with multi-provider functionality http://www.ist-muse.org/Deliverables/TF3/MUSE_DTF3.4_v17.pdf, 2007.

- Key Distribution: how to minimize the number of keys and the size of the ciphertext for the intended access control policy
- Revocation: how to handle a revocation of an access right

In this paper, we will particularly address these two problems for the smart grid data intermediary.

Policy Implementation

Attribute-Based Encryption

We propose to use attribute-based encryption (ABE) for the encryption of data. As in identity-based encryption (Boneh and Franklin, 2003) in ABE, any string can be used as a public key to encrypt. The difference is that in ABE one can use multiple keys to encrypt and be required to decrypt. In particular, one can require the private keys for a formula on the attributes. This formula then implements the access control policy.

The literature distinguishes between ciphertext-policy (CP) and key-policy (KP) ABE. In CP-ABE the formula is specified during encryption, whereas in KP-ABE the formula is specified during key generation. We recommend using the CP-ABE scheme of (Bethencourt et al., 2007).

This ABE scheme consists of the following four algorithms

- SETUP: It generates public parameters and a master key. The public parameters are distributed to all participants, whereas the master key is kept a key-managing authority, i.e. the grid regulator.
- ENCRYPT: On input of a message, the public parameters and a formula of attributes it outputs a ciphertext.
- KEYGEN: On input of the master key and a set of attributes it outputs a private key. This operation is performed by the key-managing authority.
- DECRYPT: On input of a ciphertext, the public parameters and a private key it outputs the message if the formula of attributes used to encrypt the ciphertext is satisfied by the private key.

In CP-ABE "logical and" ($\wedge$) and "logical or" ($\vee$) are the allowed operators in the attribute formulas. This somewhat limits the implementable formulas and policies compared to other implementations (Ostrovsky et al., 2007), but we argue that this is sufficient for the policies found in the smart grid. Our argument is based on the observation that policies in the smart grid usually concern a small (in comparison to the number of households) subset of permitted subjects, such that is efficient to specify this set using disjunctions, but without negations.

We use the algorithms of CP-ABE to implement a secure data intermediary. The smart meters encrypt the data using specific attributes. Note that this encryption guarantees confidentiality and privacy of the smart meter readings (protection against curious smart grid players) which is orthogonal to the integrity required for billing (protection against malicious customers). Therefore, the encryption of the (signed) smart meter readings may be performed outside the constrained smart meter, e.g. on a household personal computer. A trusted key-managing authority performs the setup of the system and then issues the decryption keys to the appropriate market participants. In practice, there are plentiful choices for such a key-managing authority. It can be played by a regulator or by a consumer protection authority. The market participants can then access and decrypt their authorized data at the data intermediary.

We emphasize the security advantages of this implementation. The market participants are bound to the policy specified by the attributes of the smart meters, i.e. the smart meter owners have assurance that their policy is enforced. The data intermediary is untrusted with respect to confidentiality and privacy. A break-in or malicious administrator at the data intermediary cannot access the plaintext data, but only the ciphertexts.

	Our Architecture
Identification	We store all data with identification. Anonymization is orthogonal to our approach, but is inherently limited in the smart grid, since already the profile is personally identifiable.
Leakage	We employ the data minimization principle in order to avoid excessive data storage.
Misappropriation	We assume that the entities in the smart grid market fulfill certain purposes and bind the purpose to those entities.
Inference	We reveal the raw data as measured by the smart meters and our architecture does prevent inferences of additional data, e.g. household habits. Randomization is orthogonal to our approach, but inherently limits the usefulness of the data.
Unauthorized Use	In our architecture the user specifies the policies. Assuming correct implementation only authorized use is possible.

Table 2: Privacy Risks Addressed By CP-ABE

Privacy regulation assumes the appropriate, approved and necessary use of personal data. Table 2 summarizes the privacy risks violating these principles in a smart grid and shows how our implementation using CP-ABE addresses these. We rely on the data minimization principle using encryption-enforced access control. We assume a structure of the smart grid market where certain actors fulfill certain purposes. Furthermore, we reveal raw data and do not prevent any inferences on the behalf of legitimate data users.

Smart Grid Intermediary

We investigate the types of policies for a smart grid intermediary and propose how to best implement them using CP-ABE. Particularly, we address the remaining challenges of key distribution and revocation algorithms. We write $\{x\}_A$ for the encryption of plaintext x using attribute A in the ABE scheme. We write *A-"type"* for an attribute with name *type*. Let *s* be the smart meter reading data.

Direct Contractual Relationship

The household maintains a number of direct contracts, e.g. with the utility supplier, that require access to its smart meter data. For example, the retailers need smart meter data to compute the customer's bill. We envision the implementation of encryption-enforced access control as follows:

- Key Distribution: The contractor supplies an identifying string as public key to the household. The household encrypts the data using this string as attribute.
- Revocation: Once the contract is dissolved, the household changes its attribute formula to encrypt, such that it no longer contains the attribute of the old contractor.

The encryption is performed as $\{s\}_{A\text{-}\text{“contractor”}}$.

Indirect Contractual Relationship

The distribution service operator maintains a number of contracts regarding the household. We call such a contract an indirect relationship between the contracted party and the household. For example, the smart grid operator may employ a demand response aggregator that helps stabilize the energy demand. The types of these contracts are commonly strictly regulated, i.e. there is a fixed number and type of them. We can therefore build a dictionary of these types and assign them attributes. Furthermore, we assume that contracts are managed on a schedule, i.e. they are closed and renewed for fixed periods. Then, we recommend implementing encryption-enforced access control as follows:

- Key Distribution: The household encrypts its smart meter data with the type of contract (e.g. "demand response") and period (e.g. "May 2012"). The smart grid operator maintains the contracts and the key-managing authority issues keys for the type of contract to its contractors and then incrementally for each period.
- Revocation: Once the contract is dissolved the key-managing authority no longer issues the keys for subsequent periods. There is no need to change the policy for the household.

The encryption is performed as $\{s\}_{\text{A-"contract-type"}\wedge\text{A-"contract-period"}}$.

Purpose-Bound

The household may volunteer its data for a certain purpose, e.g. it may consent to differentially private statistical analysis. We again assume that there is a fixed number and type of these purposes. We built a dictionary of these, such that they can be changed at will and flexibly adapted to the needs. Furthermore, commonly, the executor of this purpose is given only one-time access to the smart meter data, i.e. when revoking the access it must revoked even for data where it has been previously granted. Then we propose implementing encryption-enforced access control as follows:

- Key Distribution: The household chooses the purposes it is willing to participate in. It looks up the key (e.g. "statistics_12") for this purpose at the key-managing authority in regular intervals (e.g. once a day). Then it encrypts the data with this key. In addition, it encrypts the formula (including the attributes) it uses to encrypt using a special key for re-encryption (e.g. "reencrypt"). The key-managing authority issues private keys for a purpose.
- Revocation: Once the executor of a purpose is changed, the key-managing authority updates its keys and the households encrypt using a different attribute. Furthermore, the key-managing authority decrypts all ciphertexts (e.g. using the private key for the purpose) and all access formulas (using the private key for the special key "reencrypt"). It then re-encrypts all data using the attribute formulas, but replacing the purpose key with the new one. The executor of the purpose can then no longer access the data, even if it keeps the key.

The encryption is performed as $\{s\}_{\text{A-"purpose"}}$, $\{\text{A-"purpose"}\}_{\text{A-"reencrypt"}}$.

Policy Combination

Of course, in a realistic scenario, the household maintains multiple relationships with several market participants in a deregulated market. In order not to create a ciphertext for each relationship (and use huge amounts of storage space), we need to combine the different policies above into one ciphertext. Fortunately, this is possible using the "logical or" operator. For example, we can combine the above three examples as

$$\{s\}_{\text{A-"contractor"}\vee(\text{A-"contract-type"}\wedge\text{A-"contract-period"})\vee\text{A-"purpose"}},$$

$$\{\text{A-"contractor"}\vee(\text{A-"contract-type"}\wedge\text{A-"contract-period"})\vee\text{A-"purpose"}\}_{\text{A-"reencrypt"}}.$$

All policies will then result in formulas in disjunctive normal form which are perfectly supported by the CP-ABE scheme.

Implementation

CP-ABE relies on elliptic curves and bilinear maps for its operation. It therefore comes with even stricter performance constraints than asymmetric cryptography. Furthermore, the size of a ciphertext increases with the length of a policy. This is particularly challenging, since data packets – individual smart meter readings – are very small. We therefore need to restrict the use of CP-ABE to the minimum extent possible in order to control storage and computation requirements.

We evaluated a prototypical implementation of our scheme based on the CP-ABE implementation of (ACSC, 2012). For data size we extracted the payload from DLSM/COSEM (D.U. Association, 2011). The basic insight behind our encryption method is that the policy for encryption changes significantly less frequently than the delivery of smart meter readings. Many subsequent smart meter readings are

encrypted under the same policy. We apply the same technique as in asymmetric cryptography. The smart meter readings are encrypted using symmetric cryptography, e.g. AES 128-Bit encryption, and then the key for the symmetric encryption scheme is encrypted using CP-ABE.

We recommend the use of CBC (cipher block chaining) encryption mode for the symmetric encryption. It provides a randomization of the encryption achieving a level of security recommended by many standards. Furthermore CBC – while allowing only sequential write access – still allows random read access. Each block can be decrypted using only itself and its predecessor as input. Furthermore, we recommend aligning encryption blocks with data (smart meter readings) blocks, so that indexing and timely delivery becomes more efficient.

Each smart meter reading can be efficiently – in time and space – implemented using symmetric encryption. Each time the encryption policy changes, the household needs to choose a new symmetric key and provide a new policy data block encrypted using CP-ABE. Due to our mode of implementation, the computation and storage overhead shifts to these blocks.

Storage Overhead

We use a type-A bilinear map in an elliptic curve with field size 512 bit. This leads to element (points on the elliptic curve) sizes of 275 bytes. Each ciphertext consists of at least two elements and grows by one element for each additional policy attribute. Due to the tree construction of CP-ABE, this ciphertext expansion is independent of the logical operator (AND or OR) of the policy attribute. We can encrypt one symmetric AES 128-bit key using one CP-ABE ciphertext and only need one 128-bit (16 bytes) initialization vector for CBC. Let n be the number of attributes in the above combined policies. Then the ciphertext size is

$$275\,n + 291 \text{ bytes}$$

We emphasize that due to the use of symmetric encryption for smart meter readings, this overhead occurs only when changing the encryption policy. In the case of purpose-bound encryption, an additional block of at least 582 bytes, but usually less than 1 kbyte is required to store the encrypted policy.

Computation Overhead

We measured the computation overhead for encrypting and decrypting the policy data block using CP-ABE. Time and storage for encrypting smart meter readings is negligible. We performed our measurements on a dual-processor Xeon 2.4 GHz machine with 3.5 GB of memory. Our implementation is single-threaded, so that only one processor was used. The experimentation platform was Linux 2.6 with GCC 4.4.5. We used default compiler flags and the UNIX time command for collecting measurements. Each reported measurement result in milliseconds is the mean of 20 runs with 1000 iterations (encryptions or decryptions). We also present the bounds of the 99% confidence interval for completeness.

	Encryption		**Decryption**	
	Mean	99% CI	Mean	99% CI
1 Policy Attribute	15.75	±0.05	5.54	±0.05
2 Policy Attributes	26.65	±0.06	5.57	±0.03
3 Policy Attributes	37.48	±0.06	5.59	±0.03
4 Policy Attributes	48.42	±0.14	5.63	±0.08
5 Policy Attributes	59.26	±0.08	5.65	±0.05

Table 3: Performance Measurement in Milliseconds

Not surprisingly, the encryption time scales linearly with the number of elements in the ciphertext (plus a small constant overhead), whereas the decryption time is almost constant due to its constant use of the computationally most expensive operation of bilinear maps.

We conclude that the computational overhead is in the milliseconds which can be carried by even computational weak devices and the storage overhead is at most a few kilobytes only when the encryption

policy changes. We therefore conclude that we meet the security and trust objectives of enforcing the access control by the household (and not the data intermediary) and the functional objectives of data exchange under different relationships in a deregulated smart grid. We particularly addressed key distribution and revocation as the common drawback of encryption-enforced access control. Furthermore, our prototypical implementation underpins that the computation and storage overhead are kept at a minimum, meeting even restrictive requirements for large-scale data handling and processing.

Conclusion

Deregulated electricity markets show specific data privacy challenges since consumption data has to be exchanged in different granularity at different times between a dynamic numbers of market actors. Because smart metering is so important for integrating a large share of renewable energy sources and in this way contributing to the decarbonization of our economies, acceptance of this piece of technology is critical. While there is evidence that consumers may not always act on their privacy concerns (cp. rise of social network platforms), there is convincing data to suggest that these concerns have some impact on the acceptability and adoption of smart meters. In April 2009, for instance, protest forced the Dutch government to stop the nationwide smart meter roll-out. Moreover, privacy-enhancing technologies (PET) are still heavily discussed in the UK and the British government told the public in January 2012 that it is too early to be prescriptive about PET at this stage. In Germany, the Federal Office for Information Security organized the development of a protection profile for smart meters.

Texas, Ontario and the UK decided for a centralized exchange infrastructure for smart meters and we showed in our contribution the many advantages of communication intermediaries in deregulated markets. However, such a data broker poses both severe security and privacy issues. Our privacy-mechanism for smart grids takes into consideration the specific requirements of communication architecture with an intermediary(ies). It puts residential customers in control of their data, thereby increasing trust in the centralized exchange of their privacy-sensitive data. This ultimately lays the ground for giving each customer the ability – or at least the precondition – to decide the tradeoff between privacy and utility (the costs of lost privacy against the benefits of data dissemination) and also for giving the electricity provider the ability to incentivize the customer to participate in such a bargain by offering interesting points of tradeoff. Our solution prevents insider attacks on behalf of the data intermediary, such as the suspected invasion of thieves in the presence of residents in their homes. Technically, our approach addresses short-comings of encryption-enforced access control, such as key distribution, ciphertext size and revocation of access rights by providing tailored encryption methods for the different types of relationship in a deregulated energy market. Overall, our prototypical implementation meets even restrictive requirements for large-scale data handling and processing.

However, our approach cannot neutralize the trade-off between giving people control over their data and, at the same time, enable data-driven business models to emerge. The decisive limit is that the customer still has to trust the data receiver, i.e. the retailer, the distribution network operator or the energy service provider. Once the data is decrypted, a retailer can share the data with a third party. Also, revocation is only effective if perpetrators do not keep copies. Despite these restrictions, we present a solution to gain customers' confidence in smart metering and, by this, intend to pave the way for a new ecosystem of energy and related services.

We encourage further research in this direction. For the aspect of enforcement of policies one can research whether the power of the key-managing authority can be limited. For example, proxy re-encryption provides means to change the encryption key without intermediate decryption. This could replace our re-encryption approach for purpose-bound policies. Furthermore, for the aspect of specification of policies one can research whether data retention policies can augment our confidentiality policies. Of course, there is no known enforcement mechanism for data retention. Finally, for the aspect of management of policies the willingness and capability to specify policies by the user should be researched.

References

Al Abdulkarim, L., and Lukszo, S. 2011. "Impact of privacy concerns on consumers' acceptance of smart metering in the Netherlands," in *Networking, Sensing and Control (ICNSC), 2011 IEEE International Conference on (2011),* pp. 287 – 292.

Barenghi, A., Bertoni, G. M., Breveglieri, L., Fugini, M. G., and Pelosi, G. 2011. "Smart metering in power grids: Application scenarios and security," *Innovative Smart Grid Technologies Asia (ISGT), 2011 IEEE PES (2011)*, pp. 1 – 8.

Barringer, F. 2011. "New Electricity Meters Stir Fears", in *New York Times, January 30, 2011*, http://www.nytimes.com/2011/01/31/science/earth/31meters.html?pagewanted=all

Bethencourt, J., Sahai, A., and Waters, B. 2007. "Ciphertext-Policy Attribute-Based Encryption" in *IEEE Symposium on Security and Privacy*.

Bohli, J. M., Sorge, C., and Ugus, O. et 2010. „A Privacy Model for Smart Metering," in *Communications Workshops (ICC), 2010 IEEE International Conference on (2010),* pp. 1 – 5.

Boneh, D., and Franklin, M. 2001. "Identity Based Encryption from the Weil Pairing," SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615.

BSI (Federal Office for Information Security) 2011a. "Protection Profile for the Gateway of a Smart Metering System," (V 1.1.1 final draft, 2011, in the following: BSI-PP), https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil/schutzprofil_node.html.

BSI (Federal Office for Information Security) 2011b. "Protection Profile for the Gateway of a Smart Metering System," v01.01.01 (final draft), http://goo.gl/ow5rL.

Cho, H. S., Yamazaki, T., and Hahn, M. 2010. "Aero: Extraction of user's activities from electric power consumption data" in *IEEE Trans. Consum. Electron.,* 56(3), pp. 2011–2018.

Clauss, S., Pfitzmann, A., Hansen, M., and E. Herreweghen 2002. "Privacy-Enhancing Identity Management," IEEE Symposium on Research in Security and Privacy , IPTS Report 67, 8-16, September 2002.

DECC 2011."Smart Metering Implementation Programme: Response to Prospectus Consultation – Overview Document," p. 3, http://www.decc.gov.uk/.

D. U. Association 2011, "DLMS/COSEM: Device language message specification/companion specification for energy metering," http://www.dlms.com/organization/.

Department of Energy and Climate Change (DECC) 2010, "Toward a Smarter Future: Government Response to the Consultation on on Electricity and Gas Smart Metering," (URN 09D/524) http://www.decc.gov.uk/.

Efthymiou, C., and Kalogridis, G. 2010. "Smart Grid Privacy via Anonymization of Smart Metering Data," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on (2010),* pp. 238 – 243.

Efthymiou, C., and Kalogridis, G. 2010. Smart grid privacy via anonymization of smart metering data. *IEEE SmartGridComm'10,* pages 238–243.

Fan, Z., Kulkarni, P., Gormus, S., Efthymiou, C., Kalogridis, G., Sooriyabandara, M., Zhu, Z., S Lambotharan, S., and Chin, W. H. 2012. "Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities," in *Communications Surveys & Tutorials, IEEE (2012)*. Vol. pp. (99) pp. 1 – 18.

Federal Network Agency (Bundesnetzagentur) 2011. "Smart Grid und Smart Market - Eckpunktepapier der Bundesnetzagentur zu den Aspekten des sich verändernden Energieversorgungssystems," http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Energie/Sonderthemen/SmartGridEckpunktepapier/SmartGridPapierpdf.pdf?__blob=publicationFile.

Fehrenbach, K. 2012. "75% of U.S. electric meters will be smart by 2016," 5.3.2012, quoting Berg Insight, http://gigaom.com/cleantech/75-of-u-s-electric-meters-will-be-smart-by-2016/.

Garcia, F., and Jacobs, B. "Privacy-friendly energy-metering via homomorphic encryption," in *6th Workshop on Security and Trust Management (STM).*

Gong, S., and Li, H. 2011. "Anybody home? Keeping user presence privacy for advanced metering in future smart grid," in *GLOBECOM Workshops (GC Wkshps), IEEE (2011),* pp. 1211 – 1215.

Hevner, A., March, S., Park, J., and Ram, S. 2004. "Design Science Research in Information Systems," in *MIS Quarterly* (28:1), pp. 75-105.

Hildenbrand, S., Kossmann, D., Sanamrad, T., Binnig, C., Färber, F., and Wöhler, J. 2011. "Query Processing on Encrypted Data in the Cloud," *in Technical Report 735,* Department of Computer Science, ETH Zürich.

Jawurek, M., Johns, M. and F. Kerschbaum 2011b. "Plug-In Privacy for Smart Metering Billing" in 11th

Privacy Enhancing Technologies Symposium (PETS).

Jawurek, M., Johns, M. and K. Rieck 2011. "Smart metering de-pseudonymization" in 27th Annual Computer Security Applications Conference (ACSAC).

Kalogridis, G., Cepeda, R., Denic, S.Z., Lewis, T., and Efthymiou, C. 2011. "ElecPrivacy: Evaluating the Privacy Protection of Electricity Management Algorithms," S*mart Grid, IEEE Transactions on (2011),* Vol. 2 (4), pp. 750 – 758.

Kalogridis, G., Efthymiou, C., Denic, S. Z., Lewis, T. A., and Cepeda, R. 2010. "Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures," in *Smart Grid Communications (SmartGridComm), First IEEE International Conference on (2010)*. pp. 232 – 237.

Kalogridis, G., Zhong F., and Basutkar, S. 2011. "Affordable Privacy for Home Smart Meters," in *Parallel and Distributed Processing with Applications Workshops (ISPAW), 2011 Ninth IEEE International Symposium on (2011),* pp. 77 – 84.

Khouri, P. E., Busnel, P., Giroux S., and Li, K. 2009. "Enforcing security in smart homes using security patterns," in *Int. J. of Smart Home, 2009,* vol. 3, no. 2, pp. 57-70. http://www.sersc.org/journals/IJSH/vol3_no2_2009/5.pdf.

Khoury, P. E., Busnel P., Giroux, S., and Li, K. 2009. "Enforcing Security in Smart Homes using Security Patterns," in *International Journal of Smart Home*, Vol.3, No.2, http://www.sersc.org/journals/IJSH/vol3_no2_2009/5.pdf .

Kim, Y., Ngai, E., and Srivastava, M. 2011. "Cooperative state estimation for preserving privacy of user behaviors in smart grid," in *2nd IEEE International Conference on Smart Grid Communications,*.

Lam, H. Y., Fung, G. S. K., and Lee, W. K. 2007. "A novel method to construct taxonomy electrical appliances based on load signatures," in *IEEE Trans. Consum. Electron*, vol. 53, no. 2, pp. 653–660.

Laughman, C., Lee, D., Cox, R., and Shaw, S. 2003. "Power Signature Analysis," in *IEEE Power and Energy Magazine,* pp. 56–63.

McDaniel, P., and McLaughlin, S. 2009. "Security and privacy challenges in the smart grid," in *IEEE Security & Privacy,* 7(3), pp. 75–77.

Miklau, G., and Suciu, D. 2003."Controlling Access to Published Data Using Cryptography," in *29th International Conference on Very Large Data Bases (VLDB).*

NIST 2010. "Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid," NISTIR 7628, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.

Ofgem 2011. "Customer Engagement with the Energy market - Tracking Survey," 2011. http://www.ofgem.gov.uk/Markets/RetMkts/rmr/Documents1/IpsosMori_switching_omnibus_2011.pdf.

Ostrovsky, R., Sahai, A., Waters, B. 2007. "Attribute-Based Encryption with Non-Monotonic Access Structures" in 14th ACM Conference on Computer and Communications Security (CCS).

Pallas, F. 2012. "Data Protection and Smart Grid Communication – The European Perspective," to appear in *Proc. of the 2012 IEEE PES Innovative Smart Grid Technologies Conference.*

Quinn, E. 2009. "Privacy and the new energy infrastructure," in *Social Science Research Network (SSRN).*

Rajagopalan, R., Sankar, L., Mohajer, S., and Poor, H. J. 2011. "Smart meter privacy: A utility-privacy framework," in *Smart Grid Communications (SmartGridComm), IEEE International Conference on (2011).* pp. 190 – 195.

Ramchurn, S., Vytelingum, P., Rogers, A., and Jennings, N. 2012. "Putting the 'Smarts' into the Smart Grid: A Grand Challenge for Artificial Intelligence," in *Communications of the ACM*, 55, (4), pp. 86-97.

Ravens, S. 2010. "Great Britain Smart Meter Infrastructure: Analysis of Potential Architectures; The success of smart metering relies on distributed intelligence and a strong and flexible DCC," in *OVUM White Paper*, http://goo.gl/Od2Sx.

Rial, A. and Danezis, G. 2011. "Privacy-Preserving Smart Metering", in ACM Workshop on Privacy in the Electronic Society (WPES).

Strüker, J., and van Dinther, C. 2012: "Demand Response in Smart Grids: Research Opportunities for the IS Discipline," in *Proceedings of 18th Americas Conference on Information Systems,* Seattle, USA. Forthcoming.

Strüker, J., Weppner, H., and Bieser, G. 2011. "Intermediaries for the Internet of Energy – Exchanging Smart Meter Data as a Business Model," in *ECIS 2011 Proceedings*. Paper 103.

http://aisel.aisnet.org/ecis2011/103.

Task Force Smart Grids 2011. "Expert Group 2: Regulatory recommendations for data safety, data handling and data protection," http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf.

Varodayan, D., and Khisti, A. 2011. "Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage," in *Acoustics, Speech and Signal Processing (ICASSP), IEEE International Conference on (2011)*, pp. 1932 – 1935.

Walawalkar, R., Fernands, S., Thakur, N. and Chevva, K. 2010 "Evolution and current status of demand response (DR) in electricity markets: Insights from PJM and NYISO", in: Energy vol. 35 (4) pp. 1553-1560.

Wicker, S., and Thomas, R. 2011. "A Privacy-Aware Architecture for Demand Response Systems," *System Sciences (HICSS)*, 44th Hawaii International Conference on, pp. 1 – 9.

Yan, Y., Qian, Y., and Sharif, H. 2011. "A Secure Data Aggregation and Dispatch Scheme for Home Area Networks in Smart Grid," in *Global Telecommunications Conference (GLOBECOM 2011), IEEE (2011)* pp. 1 – 6.