Data security issues on metering systems of energy consumption in Brazil

Gislaine Midori Minamizaki [1]
Keiko V.O. Fonseca [2]
Sebastian Clauß [3]
Elke Franz [3]
Stefan Köpsell [3]
Horst Lazarek [3]

[1]**UNIFEI**
gislainemidori@gmail.com

[2]**UTFPR**
keiko@utfpr.edu.br

[3]**TU Dresden**
sebastian.clauss@tu-dresden.de
elke.franz@tu-dresden.de
stefan.koepsell@tu-dresden.de
horst.lazarek@tu-dresden.de

Abstract: In Brazil, energy consumption data of home users is mostly gathered on a monthly basis collected "in loco" by company personnel at customer premises. New features of automatic meter reading (AMR) and advanced metering infrastructure (AMI) can make consumption data readily available to both, users and providers, but pose several challenges of securing collected data. In order to earn trust and build confidence of customers, automatic meter systems should ensure data protection and fulfil security requirements. The strong regulation about citizen privacy in Germany lead to some interesting approaches to technology developments in this specific area. This paper discusses some security issues critical to AMI systems, developments aimed at data protection, privacy preserving on smart meters and relate them to Brazilian regulations of energy meter systems.

Keywords: Smart grid, AMI, smart meters, security and privacy issues, regulations.

1 Introduction

Smart grid is used to describe the integration of power, communications, and information technologies for an improved electric power infrastructure serving loads while providing for an ongoing evolution of end-use applications [1]. On its path to smart grid deployment, system designers are concerned with assuring a smooth transition from a possibly energy-inefficient and proprietary system to an open system, with highly dynamical data about power generation and consumption profiles [66] being used to control interconnected power systems. Moreover, smart grid as a critical infrastructure presents special requirements with respect to security, privacy, robustness, and survivability.

One of the steps to a smart grid is the roll-out of smart meters[1] at customer premises as part of automatic meter reading (AMR) systems. The roll-out of smart meters in several countries turned out to be not so simple: customers have been complaining of lack of transparency about services provided (e.g., Time-of-Use, TOU), costs, and data privacy [2] [3]. In Brazil, initial goals for utilities when installing AMR were to mitigate electricity theft and allow remote meter reading and remote actuation. Lessons were learned from its use: AMR caused an increase in regular bill payments, decrease in energy customer demand, decrease of accidents related to illegal wiring [4][5] but, also an increase in complaints related to measurement errors and lack of information about real time energy consumption [6][7][8]. These facts motivate studies about regulation impacts on AMR deployments and reveal challenges to the roll-out of this technology in Brazil [9][10].

Security of smart meters is a concern of many players: customers, industry, utilities, government among them. While privacy and billing fairness play an important role for customers, utilities are also interested in correcting data to efficiently manage their services, protecting their assets and keeping competitive in the market. Government concerns are about ensuring the operation of critical infrastructures while industry needs refer to the trade off between costs and a specified security level. Those are a few examples of how wide the range for security requirements can be. Therefore, a clear identification of players and their security requirements is needed to establish successful policies and standards aimed at supporting a sustainable evolution of smart grids.

Security management includes risk management, information security plans and policies, procedures, standards, guidelines, baselines, information classification, security organization, and security education [11]. A systematic approach for the design and implementation of a cyber-security programme for smart grid should be adapted to meet the business and security protection needs of each organization or application. Each organization should develop a cyber-security strategy for the implementation of its portion of the overall security programme [11].

Privacy relates to the right to "informational self-determination", that is, a citizen has the ability to determine the uses of its personal information [12]. For example, in Germany, as an explicit constitutional right, citizens can control if and how their information can be obtained and used [13]. One typical approach for preserving privacy is to limit the control and storage of data that can be considered personal by using the principle of "data minimization", which means aiming at minimizing the personal data needed

[1] Throughout this paper, this term will refer to electrical energy meter, unless stated otherwise.

to be disclosed to third parties. Even doing that, the customer has to trust in all players involved in the information processing path (data gathering, transmitting, processing, storing, etc.). This confidence is difficult to gain [14] and data protection certainly imposes additional costs.

Having in mind security and privacy issues in the smart grid context, the new distributed intelligence should be designed and implemented to provide data protection on the several data processing units and on the communication system that compose the power system [15]. Assuming the National Institute of Standards and Technology (NIST) conceptual model [16], the interconnection of the seven domains (Bulk Generation, Transmission, Distribution, Customer, Markets, Service Provider and Operations) of a power system requires a highly-distributed and hierarchical system, as an integrated set of data networks. These data networks are not homogeneous in terms of technologies but chosen to meet data transfer requirements imposed by several types of applications or environments. For example, data transfers among electrical energy distribution and operation centres deal with large amounts of data and require high-performance communication networks usually deployed as optical communication (physical layer). On the other hand, data transfers from meters used for billing purposes are usually based on short messages, periodically sent to a server. Examples of physical layer technologies [17] supported by meters are wireless (M-Bus, IIR, Zigbee, WiFi, LTE, GSM, proprietary, etc.) and wired (DSL, PLC, CSMA and extensions, fibre or proprietary, etc.).

The communication services and protocols implemented to support smart grid applications should be carefully assessed in terms of data protection and security. The privacy and security solutions should not compromise meeting the mandatory smart grid requirements of continuous operation. Figure 1 presents a pictorial example of connections (data, energy flow) of a distribution system and some possible vulnerabilities targeted by cybercriminals.

This work intends to contribute with a discussion about possible approaches to develop or apply new technologies as well as subsidize regulators and players to harmonize national and possibly international standards related to security and data protection in smart metering systems. Our particular focus is the standards/technologies aiming at the AMI roll-out in Brazil. The perspective of the European experience enlightened some interesting points about data protection and security to smart meters.

The paper is structured as follows: section 1 establishes the context whereby smart meters and their security issues will be approached; section 2 presents some smart meter roll-out experiences worldwide including Brazil and section 3 presents some concepts needed to understand the contributions of this paper. Brazilian regulations about energy metering system, data security and privacy, and main players are presented in section 4. Section 5 brings a discussion and conclusion about the aforementioned themes.

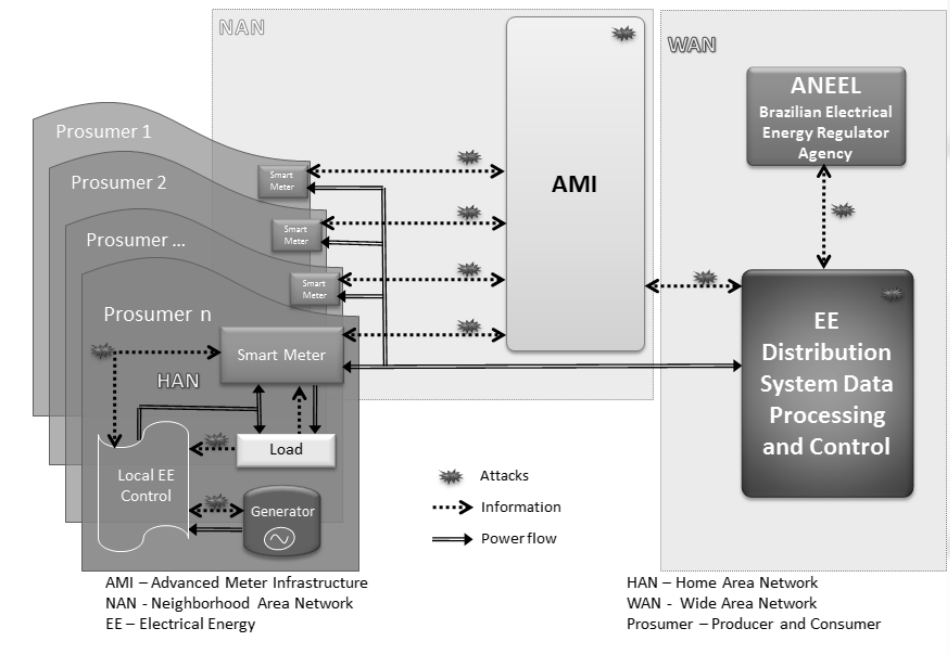

Figure 1: Example of connections and possible vulnerabilities points.

2 Smart meters worldwide

Diverse motivation for smart grid implementation can be found worldwide. The European Union focus is related to the use of renewable energy electricity, saving of energy consumption and replacement of at least 80% of traditional meter by smart meters by 2020 [19]. Although there is a common target for the deployment of intelligent metering systems in all EU member states, the development is quite diverse, with different countries applying different approaches in terms of market model, technologies, and objectives. So far, only two countries have completed a full roll-out of smart metering systems, namely Italy and Sweden, and in both cases the degree of smartness of the metering systems tends mostly to remain on the level of remote meter reading. Some countries have not considered smart metering at all, whereas in other countries the whole idea is subject to a very broad and public discussion, as for instance in the Netherlands where data privacy issues toppled the attempt to have a mandated roll-out [20].

In charge of the smart meter roll-out in Germany is the "Bundesministerium für Wirtschaft und Technologie" (BMWi, Federal Ministry of Economics and Technology). The definition of the security technical details for the smart meter system is a task of the "Bundesamt für Sicherheit in der Informationstechnik" (BSI, the Federal Office of Information Security): a protection profile (PP) (or common criteria) for smart meter gateways and security module is under development. Also a task of the BSI is the development of a technical guideline (TR 03109) which describes how the communication related details of the whole smart meter infrastructure have to be implemented to provide security and interoperability.

In the United States, nearly 5 million homes have smart meters, digital electricity gauges equipped with wireless communication. According to the Institute for Electric Efficiency, about 65 million smart meters will be working in american homes by 2020 [21].

In Asia, the installed base of smart meters in China will reach 377 million by 2020, growing from 139 million in 2012. The penetration rate for smart meters will reach 74 percent in the same year. [22]. The Japanese government wants about 80% of nationwide electricity consumption to be covered with smart meters by 2017 [23]. In South Korea, they plan to install smart meters in all homes by 2020 [24].

Brazil already has a clean energy matrix and is the second largest producer of hydroelectricity in the world (after China) [25]. Thus, Brazilian motivations for smart grid are related to a better Quality of Service (QoS) provisioning and non-technical losses reduction. These losses are mainly related to theft and are very high compared to global levels [26]: they include meter tampering, violation and/or modification of gear teeth on mechanical meters, stealing of digital meters (wiring violation), stealing of energy directly from the distribution network wiring, among others [5]. In Brazil, a typical AMR system with anti-fraud features uses a gateway that collects data from several energy meters and forwards to the utility as well as receives and places commands to switch-on/off energy supply (remote actuation, or remote service connects or disconnects). The gateway and energy meter sensors are placed out of reach of the consumer but an end user can display its energy consumption on its premises through a device connected to the energy meter, wireless or by power line communication (PLC) [5][27][28]. This technology is also useful to hard-to-access locations and paves a path to implement prepaid energy for low income customers, an important step to encourage them to learn how to control (or be aware of) their energy consumption [29]. Nevertheless, the technology itself does not solve the problem: education and information must be provided to the public to avoid stealing recurrence. As also reported, recurrence occurs on 40% of the cases where no clear information about energy charges and power consumption is given [5]. An average reduction of the previous energy demand is perceived once the ex-illegal consumer is correctly charged [4]. Section 4 approaches specifically the Brazilian context for smart metering roll-out.

It is interesting to point out that differently from Brazil, where the billing period for a domestic customer is one month, in EU countries the electricity billing period is usually related to a contract (in Germany it can be as long as one entire year, in UK 3 months, in France 2 months, etc.). The feedback on energy consumption clearly affects the energy awareness of the customer [30]. Smart meters, if designed to provide a meaningful display of the energy consumption, could increase customer awareness about TOU, tariff periods, etc., clearly impacting on sustainability goals.

3 Security and privacy issues in the smart grid

Enforcing security and privacy issues is of vital importance for a broad acceptance and, hence, a successful deployment of the smart grid. Security requirements are usually defined by means of protection goals. The basic protection goals are confidentiality, integrity, and availability. Particularly, confidentiality and integrity of the data in the smart grid are of high importance; only authorized persons should be able to access the data, and unrecognizable modifications of the data have to be prevented. The protection profile defined by BSI [31] focuses on confidentiality and integrity since the smart grid has to be designed in a way that ensures its functioning even if smart meter gateways fail.

To prevent possible attacks, it is also important to ensure that the origin of messages can be verified, i.e., to ensure the authenticity of data. Integrity and authenticity is required for billing data as well as for data regarding the load situation and for controlling data sent within the smart grid. Furthermore, auditing is relevant for checking events occurred; e.g., security relevant events, but also transmission of relevant billing information should be logged.

While data security refers to all kind of information, data protection or privacy refers to personal information. Detailed information about energy consumed by the customer arising in the smart grid can imply serious privacy risks. Information about energy usage reveals the absence of users. Moreover, several investigations have shown that detailed information about consumer habits can be derived from such information [32].

Given these potential threats, a thorough security analysis and the introduction of appropriate security measures are indispensable for the smart grid. Due to the scale of data volume to be collected and processed at a smart grid (for example, a large number of devices generating data over small time intervals), the process of analysing data for security reasons is classified as a big data problem. Since many smart grid applications have stringent real time requirements, the additional processing overhead imposed to cope with security policies should be considered on real time scheduling analysis, as pointed out in [35]. The following section will only highlight some security problems on the example of smart meters and communication to illustrate possible problems.

3.1 Smart meter

A traditional electromechanical meter presents the value of the accumulated consumed energy over a large time period. This information does not allow any conclusion on variations of consumption over time since the last meter reading. Modern electronic solid state meters are able to measure the load over time, process the data, submit it and receive and process data as well, e.g., requests for actual meter data, tariff information, commands for a remote (dis)connection and/or load limitation, firmware updates, etc. This data can be transmitted from the metering device (or the associated communication module) and the back-end energy distribution management system through a data network.

New features of AMR and AMI are: automatic processing, transfer, management and utilization of metering data plus automatic management of meters. According to [17], these systems should provide 2-way data communication with meters and meaningful and timely consumption information to the relevant actors and their systems, including the energy consumer. It should also support services that improve the efficiency of energy consumption and of the energy system (generation, transmission, distribution and especially end-use). Other examples of meter features are prepaid energy, ability to provide immediate response to power shortages, ability to meter energy in both ways (at prosumers[2]), report generation, etc.

Although an AMR/AMI system makes consumption data readily available, it also poses several challenges for securing the collected data. The AMR/AMI information infrastructure requires a reliable communication to achieve the desired results: it should be secure for customers, ensure that personal data will not be collected and misused by third parties, that measurements will reflect the correct energy consumption, while responding timely to many conditions in energy supply and demand. In addition. it should be secure for utilities in order to guarantee that energy consumption measurements are correct and no theft exists.

Vulnerabilities and threats are security aspects that need to be considered early in the application development process [1]. Idaho National Laboratory (INL) [18] reported that security solutions for meter systems are not trivial due to their scale and the lack of knowledge of their behaviour under undesired conditions, for example, cyber-attacks.

Smart meters at customer premises must consider technologies that resist physical tampering of meters or violation of embedded software and hardware: metrology aspects in the implementation of the metering system should have their protection considered in the meter model approval process. The system should be submitted to the approval process of a national metrology entity that certifies that the whole path of measurement information flow, starting at its generation and ending at the consumer exhibition, that is, the legally relevant chain, preserves the correct value of the measurement. In Brazil, the requirements related to the meter software were set according to the European Cooperation in Legal Metrology (WELMEC 7.2) and International Organization of Legal Metrology (OIML) as summarized in Table 1 [6]. Besides these requirements, validation evidences are also required from the meter manufacturer. These evidences should provide detailed description of the used techniques in the software validation process, together with the results of the implemented tests. They were aimed at controlling new software releases or software updates (correction of known errors, enhancements, etc.) to assure their compliance to the approved software.

Table 1: Meter software requirements. Adapted from [33].

Item	Meter Software Requirements
Embedded software	software identification, user and communication interfaces and protection against changes;
Data transmission	completeness, integrity, authenticity, confidentiality of keys, handling of corrupted data, delay and availability of transmission service;
Software Separation	distinction of legally relevant software and not relevant, protective software interface and mixed indication;
Download of legally relevant software	software releases and/or updates control;
Fault recovery	authentication, integrity, software traceability and download consent;
Adequacy of the device display	clarity and completeness, meter parameter configuration;
Dynamic behaviour	data display update (e.g., in regular time intervals).

In Brazil, the approval process of an electrical energy meter requires from the manufacturer the disclosure of the legally relevant software (source code) to the national metrology agency (Brazilian Metrology, Quality and Technology Institute - INMETRO). As described in [33], the evaluation is based on the software documentation and a careful checking of the data flow over the entire legally relevant chain. The evaluation checks if security/safety requirements are met and applies test cases. The provided software documentation allows for consistency checking and tracking of legal relevant variables. The test cases include also vulnerabilities scanning. The analysis of the source and object codes does not guarantee that the provided

[2] Prosumers: producer and consumer.

executable code refers to the version approved. The mapping of the expected behaviour described in a source code language should be checked against the available executable code. A process called "software integrity verification" should be able to identify the approved software version among distinct versions based on cryptographic schemes. Without approval of the national metrology agency, an electrical energy meter model cannot be used for billing purposes.

In order to deserve customer trust, each new feature or software update on a specific meter model should be free of bugs which can lead to potential measurement errors and/or security breaches. The updates should also be validated by metrology agencies as trusted solutions, therefore requiring each time the process of software integrity verification, a very laborious and time-consuming task, which may even lead to security problems itself, as it makes timely updates for security-critical bugs more difficult. One typical approach to circumvent this problem is to keep the core functionality which requires certification very small, and therefore easier to certify [33]. Further, trusted platform module (TPM) and similar approaches can be used to verify that the software running on a meter is certified.

3.2 Communication systems

To some extent, smart grid communication requirements are comparable to those found on industrial communication networks, for example, industrial control, supervisory control and data acquisition (SCADA), distributed control (DCS) and/or process control (PCS) systems. Communication systems designed to match industry requirements, as well as those meant for power systems, had been mostly based on closed proprietary solutions. One claimed reason for proprietary solutions was the thesis that limited availability of open documentation (all under the control of the solution provider) would lead to a higher level of data protection, which is not true [34]. Nowadays, the industry and power system communication deployments are moving to open standards: the immediate benefits are better interoperability and cost reduction through more choices of solution providers and a wide knowledge base shared among users. Closed protocols or not, a smart grid communication subsystem must be designed to avoid security breaches: data transmissions are subject to eavesdropping, jamming, data interception and/or modification, transmission delays or transmission blocking. Independent of the physical layer technology, protocols or provided services, a data network of a smart grid should have its robustness assessed against data and privacy protection. Mostly standardization bodies consider security as strongly dependent on authentication, authorization and privacy technologies [35].

Although there exist several legacy cyber security techniques developed for enterprise and home networks, smart grid presents quite diverse communication requirements which make reuse of these techniques not directly possible. To be reused or adapted, cyber security techniques for such networks should carefully consider smart grid requirements of scalability, real time performance, and continuous operation features. The main differences between an existing complex communication system (e.g., the Internet) and one aimed at smart grid communications are shown in Table 2 [35]. Other research papers have approached the engineering requirement specifications of the communication support needed in a smart grid [36][37].

Table 2: Differences between the internet and the smart grid communication network. Adapted from [35].

	The Internet	**Smart Grid Communication**
performance metric	throughput and fairness	message delay
major traffic	power law (large amount of aperiodic traffic)	mainly periodic like measurements, sensor readings. Alarms
timing requirement	delay sensitive (100ms), jitter sensitive (soft real time requirements) to best effort	time-critical to best effort
communication model	mostly end-to-end	two way, limited Peer-to-Peer, heterogeneous
protocol stack	IPv4, IPv6	proprietary, heterogeneous, IPv6

The application of security mechanisms in smart grid communication networks may require deployments on several communication layers: firewalls, virtual private networks, IPSec technologies, Secure Shell, SSL/TLS, etc. The security problem on smart grid has been approached in several research papers: [38] characterize cyber attacks on smart grids based on temporal anomalies; [39] presents a security model to AMI and methodologies based on a quantitative information-based exposure metric to evaluate the completeness of implemented security mechanisms; [40] consider the use of Petri modelling of large infrastructures of smart meters to represent coordinated cyber-physical attacks on smart grids; [41] studies about smart grid protection against cyber attacks. This last paper approaches the problem of moving from a proprietary architecture to an open and interconnected automation platform and the major security challenges to overcome.

Solutions to increase security of a smart grid communication infrastructure, whatever they are, should take into account system reliability, for example, hard real time requirements of smart grid applications should not be violated [42]. Although solutions based on usual Internet protocols (TCP/IP) are very appealing [43], they are not meant to support real time requirements of energy systems. These particularities of smart grids, besides the motivation of independence of proprietary/closed solutions/equipments, lead users, service providers and energy/equipment suppliers to join efforts to specify open communication protocols [44][45], following similar efforts of manufacturing and control process automation. The specifications for such a communication system have been difficult to develop, however, because it needs to support a great variety of applications, many of which have not yet been developed [46].

Of our particular interest is the communication system of a metering system aimed for billing purposes and load demand control. One typical deployment of such system is a centralized measurement system where all sensors are concentrated in one location (hub) and meter displays are at customer premises. The measurement information can be wirelessly or through wires forwarded from the hub to a node of the data distribution system. The automation of the reading process should:

- gather data periodically (monthly, weekly, each 15 minutes, etc.);
- associate this data to some specific tariff period (Time of Use -TOU, the price of the energy when it is used). The time period may or may not be updated through the communication system;
- display the actual value of consumed energy and TOU to the customer;
- provide data protection to customer data and embedded software on the meter, as well as during transfers.

Among the communication protocols already standardized to metering devices in Germany are the M-Bus and its wireless version as defined in the technical directive about security [47].

Few examples of cyber incidents targeting the meter communication systems are:

a) denial-of-service (DoS) attack exploring protocol flaws or through jamming the wireless transmission. Countermeasures for DoS attacks include frequent checking and updating of protocols. Jamming can be minimized by using spread spectrum technologies or temporal redundancy.
b) privacy violation by capturing electricity usage information in order to profile consumers [48] (eavesdropping by listening on open wireless transmission, for example). Countermeasures include the use of cryptographic solutions and simple value masking schemes [67]. Whether the procedures of secure key management are mandatory or not, a trade off with respect to cost/complexity should be carefully considered when developing key management schemes for smart grids [49].
c) metering protocols DLMS and IEC 60870-5-102 implementations: they can have functions to read metering data which do not require a password, and configuration/disconnect functions that require the operator password - making them vulnerable.
d) master-slaves implementations: a "man-in-the-middle" device can be inserted between the slave meter and its master to change measurements values, ask for or avoid remote disconnection, etc.

3.3 Security concepts

One approach to data protection known as Privacy by Design (PbD) [50][67][68] is of particular interest of the Smart Grids Task Force of the European Commission (Expert Group 2). Based on this approach, the group established recommendations for data safety, data handling and data protection [51]. Implementations guided by privacy by design principles apply so-called Privacy Enhancing Technologies (PET) defined as "a system of ICT measures protecting informational privacy by eliminating or minimizing personal data, thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system" [52] .

Among the approaches to preserve consumer privacy in smart grids are suggestions for privacy-preserving billing, e.g., by means of zero-knowledge proofs and homomorphic encryption [53] or for separating data needed for billing purposes and data necessary for power generation and distribution [54]. The rationale for the latter is the fact that billing data must be securely attached to consumers but can be collected in longer time intervals (e.g., monthly) while data necessary for load balancing is required after shorter periods but can be anonymous. Other approaches aim at obfuscating consumption data by applying aggregation and homomorphic encryption (e.g.[48] [55]).

Trusted Platform Modules (TPM) enforce specific behaviour and protect a system against unauthorized changes and attacks such as malware and root kits. The use of TPM within smart meters was suggested to ensure the authenticity of the software executed on the meters [56].

As computing has expanded to different devices and infrastructure has evolved, the concept of trusted systems extended well beyond the computer-with-a-TPM to other devices, ranging from hard disk drives and mobile phones [56].

In Germany, a protection profile specification aimed at a metering gateway as well as companion standards are on their way (the security standard is not limited to energy meter but all smart meters) [31]. The protection profile defines minimal security requirements smart meters have to fulfil. Smart meters will be verified based on this protection profile and will get a certificate confirming the fulfilment of the protection goals. Technical details regarding the implementation of the protection profile are given in the technical guideline [57].

In order to prevent unauthorized accesses by attackers from outside, only the gateway can establish a communication to an external entity. However, the gateway administrator may need to contact the gateways immediately in some cases. To ensure the reachability of the gateways the protection profile allows a so-called wake-up service: The gateway administrator can send a digitally signed and encrypted wake-up message that contains a time-stamp to the gateway. The gateway decrypts the wake-up message and verifies the signature. If the signature could be successfully verified, the time-stamp is checked; only messages sent within a certain period of time are accepted to prevent replay of messages. If the message could be accepted, the gateway initiates a connection to a pre-configured external entity.

4 Brazilian meter regulation on data security and privacy - main players

Successful roll-out of smart metering systems depends on regulatory authorities, governmental and legislative bodies.

These institutions play a significant role in assessing costs and benefits of smart metering deployments, setting up the roll-out scheme and monitoring the actual implementation. Without a clear legal and regulatory framework, market parties will be reluctant to commit themselves to the investments needed to set up a whole new communication and metering infrastructure. This would deter a smart metering roll-out and lead to inefficient results.

The legal and regulatory framework will certainly have a decisive influence on the overall costs and benefits. This is particularly true in the case of a mandatory roll-out where the framework should set the responsibilities of market parties, time schedules, new tariff schemes, and minimum functionalities. Moreover it should explain clearly how the investment and operating costs will be accommodated in tariff regulation.

In Brazil, this role belongs to Brazilian Electrical Energy Agency (ANEEL), an agency established to regulate, authorize, police and if necessary punish private authorized companies working in public service in the electricity market. Besides ANEEL, the following stakeholders also influence the referred roll-out:

The Brazilian Association of Technical Standards (ABNT) together with INMETRO are responsible for establishing the certification criteria for electronic meters and for smart grids. These players will define adequate metrology and conformance policies according to technical specifications defined by ANEEL. Among their challenges is the specification of services and protocols to be provided by the meter communication support aimed at the Brazilian market. Further, they need to provide a guarantee that the software inside the meter is exactly the one approved by INMETRO[6].

Meters manufacturers, solution providers and the Brazilian Association of Electrical and Electronics Industry (ABINEE): for those players, the roll-out of smart meters represents a new market but more security mechanisms represent increase of cost and investment in an expertise on a field not employed on the traditional meters. ABINEE sponsors a project called SiBMA (Brazilian System for Advanced Metering), whose main goal is to design and prototype a technical solution for remote controlling meters, and for automatically collecting consumption data from electricity meters in the Brazilian residential and industrial market. The project aims at developing a set of open communication protocols intended to resource limited devices. Another goal of this project is to produce a technical specification of an architecture and protocols to be submitted as a possible national standard for smart metering devices [58].

Power distribution utility companies and the Brazilian Association of Power Distribution Companies (ABRADEE), which are concerned about their economical balance: They need to evaluate, whether benefits from utilizing data of smart metering systems (e.g., profits saved by reducing electricity theft, better demand response, better distribution control, fast response to system failures, etc.) justify the necessary investments in infrastructure to support the new technology in the considered time period. In fact, electronic meters have a lifetime lower than the current depreciative rate considered by ANEEL, which poses another decisive factor to the distributor when it comes to investing in smart meters. Considering meter security aspects, they are concerned about protecting measurement data against any forgery.

Customers and the consumer protection organizations (in Brazil, PROCON): consumer resistance is probably the most difficult barrier to mitigate. Examples of consumers heavily opposing smart metering deployment can for instance be found in the United States and in the Netherlands [59]. In most cases, consumer resistance can be driven primarily by two reasons: Consumers might fear that security and privacy of data gathered by smart metering cannot be guaranteed and hence unauthorized parties might have access to private data. Consumers might also fear that they would have to bear the costs for deploying a smart metering infrastructure or that new (time-of-use) tariffs would lead to higher energy costs, whereas benefits for consumers might prove to be overestimated. Finally, depending on granularity and delay in displaying consumption information, the consumer will not have the same possibility of assessing the measurements like on an electromechanical meter. For example, with an electromechanical meter, the consumer can turn off all equipment and immediately verify if the mechanic disc of the meter stops. If it does not, there is an unknown source of consumption. Such an approach might not be possible with a usual smart meter.

Meters intended for billing purposes in Brazil must be certified by INMETRO. As far as data security is concerned, INMETRO ordinance about energy meters states: “An access protection through password should be available to block non-authorized access to programmable meters, avoiding non-authorized changes on metrological parameters and registered data file, whenever the sealing device of the optical port is not available [61].

ANEEL should provide a balance between all players in benefit of the Brazilian society. The issue is not simple: stakeholders have different needs, and furthermore, the cost of the meter must be affordable. Costs and benefits of smart metering depend on the technical specifications of the meters and the rolled-out infrastructure. In 2012, ANEEL launched a regulation for energy metering systems [59] establishing deadlines and terms for TOU implementation and electronic meters. As far as remote communication systems and security are concerned, the regulation states that If the metering system provides remote communication, the distributor should adopt procedures and technologies that assure the security of the transported data, especially those of personal individuals collected at consumer premises. The distributor is not allowed to make available any data collected from a consumer unit to third parties without the consent of the owner. Apparently, the security concern, according to the ANEEL regulation text, is based on the hypothesis of a meter system with a remote communication system. However, even without remote communication, data can be stolen directly from the meter by tampering the device and reading its memory. Also, flawed software/hardware and programming codes can also cause intentionally or not access to personal user data directly from the meter. Also, the meaning of the word “security” was not clearly defined in the aforementioned regulation. Depending on the perspective [60], security can

be interpreted differently: in communication and computing systems it usually refers to cyber-security, requiring the smart grid to be designed to defend itself from passive (eavesdropping, sniffing) and active (DoS, man-in-the-middle) attacks, for example. While in power systems, security issues comprise intentional physical attacks, (un)intentional human errors, self-system malfunction due to bugs, or severe weather affecting the system operation and energy provisioning (for example, energy dependence). In [9], the impact of regulatory intervention on Smart Meter system it is discussed from the ANEEL point of view.

5 Discussion and conclusion

Smart Grid deployments pose challenging quests towards a sustainable society. We limit our discussion to one of the first steps of this pathway: smart meters, that is, the metering device as the basic component to AMR for low voltage consumers on customer premises. We also assume the communication system for remote reading and actuation is limited to the first data concentrator that collects data directly from meters, wired powered meters, a stationary node distribution (static topology).

This paper points some approaches to be considered when designing systems to cope with modern security and privacy preserving techniques. As pointed out at section 3, by considering at design time the use of trusted platform modules not only costs but also homologation process time like that required by INMETRO can be reduced. Also, by avoiding direct enquiries to the meter from an outside network, wake-up approaches based on signed, digitally encrypted, time-stamped message can be used to provide secure data request and transfers. It is also important a careful choice of communication protocols and technologies to provide the necessary security level aimed by the application but still matching its timing requirements.

The present regulations about of smart metering systems aimed to billing purposes for the Brazilian market poses some challenges to energy distributors and manufacturers. Despite the alleged benefits of smart metering, market parties will not in all cases adopt smart metering voluntarily or willingly. Moreover, if they do aim to, their efforts may be hampered by existing barriers. For example, by now, it is hard for manufacturers and utilities to plan how many customers will opt for the new meters in which period of time – a guessing game that also depends on how informed customers will be. The literature reports [14][59] that actions to provide consumer education are crucial to successful smart metering deployments, not only to achieve energy-savings or a smooth transition to a prosumer environment, but also to secure the smart grid critical infrastructure. Despite the ANEEL regulation states that the utility is responsible to develop information campaigns [63], it is not clear if it also their duty to clarify about smart grid implementations. For example, if a customer decides for TOU he/she should be aware that the energy consumption during peak time must be avoided or his/her bill can significantly increase.

Whatever the strategy adopted for a massive rollout of meters, together with scalability, security and costs concerns, consumer's concerns should be not ignored. Currently, the topics of data integrity and tariff reduction are more discussed than security in Brazil. Advanced smart metering systems are more expensive than basic smart metering systems and the same happens to security mechanisms: more protection represents more costs. ANEEL regulation defines only minimum requirements for smart meters: further functionalities, including additional data protection and security are optional and imply additional costs. It does not mean that security is not a concern in Brazil, moreover, one has to expect that concerns will arise when the Smart Grid is deployed. Studies have revealed that consumers who claim to have the best understanding of the smart grid are the most concerned about the smart grid's impact on their privacy [64] and will be the first to argue against the lack of security. Consequently, security as a whole must be considered by design. If not, the complexity to introduce security after the implementation will lead to larger costs.

Also clear from the facts is the need of qualified IT personnel in security subjects. Again the problems posed require a decision about who should be in charge of the qualifying costs. Engineering and Computer Science schools must have their curricula adapted to include basics and higher level courses of IT security. Further, business management courses should include information security contents to prepare new generations of managers aware of the security risks of the new integrated infrastructure of smart grid. Particularly in Brazil, most consumers have none or little school background to understand IT security and/or energy basic concepts. Hence, fact sheets, consumer guides, meter displays and billing accounts, etc. should be presented in a user-friendly way in order to increase the benefits of smart grid deployments. A fully interdisciplinary team will be needed to work on these subjects.

In spite of the fact that goals for smart meter systems were somehow different depending on the country context and regulation aspects, common problems pose for consumers or companies about data on meter/gateways: how to protect its integrity? How to ensure only authorized access on it? By now, Brazilian solutions still rely on non-standardization of the communication support and a generic ANEEL regulation about it. As far as we know, in Brazil, there is no clear leader heading the discussion about security issues on metering systems. As approached by ABINEE, a relevant concern should be the interoperability between different meters, communications infrastructures and metering management systems [65]: in this sense, efforts should be taken to include major players of metering systems (gas, water) in standardization task forces to reduce biasing that could favour particular players of the metering market.

In Europe, efforts have been conducted to make better use of standards already in use providing a stable framework for metering system deployments. The mapping of actual requirements of smart metering systems to existing standards has provided a clear picture of missing points of standardization. Standardization efforts are now focusing on task forces to fulfil only these missing points instead of creating new standards.

Finally, we show that new approaches considering security should be adopted at designing metering systems. Further research is under development by the authors to assess robustness of the security solutions taking into account system scalability and real time requirements.

Acknowledgements

Keiko V. O. Fonseca received support from CNPq – Conselho Nacional de Desenvolvimento Científico e Tecnológico, Brazil.

References

[1] IEEE Std 2030™-2011, IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Application and Loads, Sep 2011.

[2] Sunshine, W. L. Do Smart Meters Pose Problems? Energy.About.com. Avaiable at: <http://energy.about.com/od/billing/a/Do-Smart-Meters-Pose-Problems.htm>.

[3] Website: Stop Smart Meters! Available at: <http://stopsmartmeters.org/2012/02/02/pay-for-your-health-pay-for-your-rights-we-say-no>.

[4] Transforming Electricity Consumers into Customers: Case Study of a Slum Electrification and Loss Reduction Project in São Paulo, Brazil, Bureau for Economic Growth, Agriculture and Trade U.S. Agency for International Development, Washington, D.C. 20523, February 2009, available at: http://pdf.usaid.gov/pdf_docs/pnado642.pdf

[5] AMPLA. Furto de Energia: o Grande Desafio da Ampla, 2010, available at: http://www.sap.com/brazil/about/eventos/sapforum2010/apresentacoes/10-03/SP1/2010.03.09%20-%20AMPLA%20Projetos%20Combate%20ao%20Furto.pdf

[6] Boccardo, D.R., et al. S., Software evaluation of Smart Meters within a Legal Metrology perspective: A Brazilian case, Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES Digital Object Identifier: 10.1109/ISGTEUROPE.2010.5638881 – 2010.

[7] Freire, W.; Public Ministry of state of Rio de Janeiro makes the judgment about action against the utility "Light" because of electronic meters. Jornal da Energia, Feb. 2012. Available at: http://www.jornaldaenergia.com.br/ler_noticia.php?id_noticia=8982&id_tipo=2&id_secao=17&id_pai=0

[8] Villela, F.; At the hearing, consumer organizations criticize the proposal Aneel prepayment energy. Agencia Brasil, September 2012. Avaiable at: <http://agenciabrasil.ebc.com.br/noticia/2012-09-19/em-audiencia-entidades-de-defesa-do-consumidor-criticam-proposta-da-aneel-de-pagamento-antecipado-de->.

[9] D.R.V.Leite, H.Lamin,J.M.C de Albuquerque, Camargo I.M.T:Regulatory Impact Analysis of Smart Meters Implementation in Brazil, IEEE 2011.

[10] Gomes, R. C., Printes, A. L., Ramos, C. M. Proposta de Sistema com Arquitetura para Implementação de uma Smart Grid na Rede de Distribuição em Baixa Tensão. III SBSE, Belém, 18-21, 2010.

[11] U.S. NIST, "Guidelines for smart grid cyber security (vol. 1 to 3) - August 2010.

[12] Virtual Privacy Office Available at: http://www.datenschutz.de/privo/recht/grundlagen/, accessed on November 10th, 2012.

[13] Eingriffe in das Recht auf informationelle Selbstbestimmung nur auf der Grundlage eines Gesetzes, das auch dem Datenschutz Rechnung trägt (Volkszählungsurteil) (BVerfG) available at http://www.bfdi.bund.de/DE/GesetzeUndRechtsprechung/Rechtsprechung/BDSGDatenschutzAllgemein/Artikel/151283_VolkszaehlungsUrteil.html;jsessionid=28FC7B50A880972DCCFD1EA0CD0D04A0.1_cid136?nn=1236576.

[14] Brand, S. A.; "Dynamic Pricing for Residential Electric Customers: A Ratepayer Advocate's Perspective", The Electricity Journal, July 2010.

[15] Yan, Y., Qian, Y., Sharif, H., Tipper, D.; "A Survey on Cyber Security for Smart Grid Communications". IEEE Comm.Surveys & Tutorials, vol. 14, nº 4, fourth Quarter 2012.

[16] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, NIST Special Publication 1108, January 2010, Office of the National Coordinator for Smart Grid Interoperability, available at http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

[17] Koponen, P. (ed.), Saco, L.D., Orchard, N., Vorisek, T., Parsons, J., Rochas,C., Morch, A. Z., Lopes, V., Togeby,M.; "Definition of Smart Metering and Applications and Identification of Benefits", ESMA Final Report, May 2008, Version 1.1, available at: http://www.esma-home.eu/UserFiles/file/downloads/Final_reports/ESMA_WP2D3_Definition_of%20Smart_metering_and_Benefits_v1_1.pdf.

[18] Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues, April 2009, INL/EXT-09-1550, INL Critical Infrastructure Protection/Resilience Center Idaho Falls, Idaho 83415

[19] Directive 2009/72/EC concerning common rules for the internal market in electricity, OJ 2009 L211. Annex I Measures on consumer protection

[20] Balmert, D.; Grote, D.; Petrov,K.: Development of Best Practice Recommendations for Smart Meters Rollout in the Energy Community, by order of: Energy Community Secretariat, Submitted by: KEMA International B.V., February 2012, available at http://www.energy-community.org/pls/portal/docs/1460178.PDF.

[21] Utility-Scale Smart Meter Deployments, Plans & Proposals, May 2012, Institute for Electric Efficiency, 701 Pennsylvania Avenue, N.W. , Washington, D.C, available at http://www.edisonfoundation.net/iee/Documents/IEE_SmartMeterRollouts_0512.pdf.

[22] Pike Research Report "Smart Grid in China", January 2013. Avaliable at http://www.pikeresearch.com/research/smart-grid-in-china.

[23] K. Bojanczyk; D. J. Leeds: "The Smart Grid in Asia, 2012-2016: Markets, Technologies and Strategies", May 2012, available at http://www.greentechmedia.com/research/report/smart-grid-in-asia-2012-2016.

[24] Stromback, J.; Dromacque, C., "Evaluation of residential smart meter policies" July 2010 available at: http://www.worldenergy.org/documents/ee_case_study__smart_meters.pdf.

[25] U.S. Energy Information Administration. Countries: International Energy Statistics. Available at <http://www.eia.gov/cfapps/ipdbproject/IEDIndex3.cfm?tid=6&pid=29&aid=12>.

[26] Pepitone da Nóbrega, A. Resultados da Audiência Pública n.o 43/2010. ANEEL, Brazil. Available at: <http://www.aneel.gov.br/cedoc/aren2012502_1.pdf>. Acessed on Oct 7th, 2012.

[27] Elster product Garnet. Available at: http://energia.elster.com.br/pt/GARNET.html, accessed on Nov 18th, 2012.

[28] SIM NANSEN - Sistema Inteligente de Medição. http://www.nansen.com.br/solucoes_simnansen.php, accessed on Dec 10th, 2012.

[29] ANEEL: Regulamentação sobre pré-pagamento de energia está em audiência pública. <http://www.aneel.gov.br/aplicacoes/noticias/Output_Noticias.cfm?Identidade=5753&id_area=90>.

[30] Darby, S. The effectiveness of feedback on Energy consumption: A review for DEFRA of the literature on metering, billing and Direct displays, Sarah Darby, April 2006, Environmental Change Inst., University of Oxford.

[31] Bundesamt für Sicherheit in der Informationstechnik: Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Version 01.01.07 - 21. December 2012 (Release Candidate). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf?__blob=publicationFile.

[32] M. Newborough, P. Augood: Demand-side management opportunities for the UK domestic sector. IEE Proc. of Generation Transmission and Distribution 146 (3), 1999, 283-293.

[33] Camara,S., Machado, R., Carmo, L.F.R.C.; "A consumption authenticator based mechanism for Time-Of-Use smart meter measurements verification" Applied Mechanics and Materials, vol. 241-244, pp. 218-222. December, 2012.

[34] Cyber Security Assessments of Industrial Control Systems Good Practice Guide - CPNI Centre for the Protection Of National Infrastructure, Homeland Security, November 2010, available at http://ics-cert.us-cert.gov/csdocuments.html.

[35] W. Wang, Z. Lu, "Cyber security in the Smart Grid: Survey and challenges", Computer Networks. January 2013, available at: http://dx.doi.org/10.1016/j.comnet.2012.12.017.

[36] Bose, A.; "Smart Transmission Grid Applications and Their Supporting Infrastructure", IEEE Trans. on Smart Grid, vol.1, no. 1, June 2010, pp. 11-19.

[37] Wang, J. ; Leung, V.C.M.: "A survey of technical requirements and consumer application standards for IP-based smart grid AMI network", in: International Conference on Information Networking (ICOIN), Jan. 2011, pp. 114 – 119, ISSN 1976-7684, ISBN: 978-1-61284-661-3.

[38] C-W.Ten; J.Hong; Chen.C.Liu: "Anomaly Detection for Cybersecurity of the Substations", IEEE Trans. on Smart Grid, Vol.2; Issue 4; pp 865 - 873, Dec. 2011.

[39] Hahn, A.; Govindarasu, M.: "Cyber Attack Exposure Evaluation Framework for the Smart Grid", IEEE Transactions On Smart Grid, Vol 2 Issue 4, pp.835-843, ISSN:1949-3053, Set. 2011.

[40] Chen, T.M.; Sanchez-Aarnoutse, J.C.; Buford, J.: "Petri Net Modeling of Cyber-Physical Attacks on Smart Grid", IEEE Trans. On Smart Grid, Vol.2 Issue 4;pp.741-749, Dec. 2011.

[41] Wei,D.; Lu,Y., Jafari, M. Skare, P.M.; Rohde, K.; "Protecting Smart Grid Automation Systems Against Cyberattacks", IEEE Trans. On Smart Grid, Vol 2 Issue 4, pp.782-795, Dec.2011.

[42] Metke, A.R., Ekl, R.L.;"Security Technology for Smart Grid Networks", IEEE Transactions on Smart Grid, Vol. 1, No. 1, June 2010, pp 99-107.

[43] T. Jin, M. Mechehoul, "Ordering Electricity via Internet and its Potentials for Smart Grid Systems", IEEE Transactions On Smart Grid, Vol. 1, No. 3, December 2010, pp 302-309.

[44] Rohjans, S., et al.; "Survey of Smart Grid Standardization Studies and Recommendations", 1st IEEE Int. Conf. on Smart Grid Communications, 2010, pp. 583 - 588.

[45] IEC61850, "Communication networks and systems in substations", IEC, 2011, available at http://www.iec.org.

[46] Anderson, D., Zhao,C,.Hauser, C.; Venkatasubramanian, V.; Bakken, D.; Bose, A.; "Intelligent Design Real-Time Simulation for Smart Grid Control and Communications Design", IEEE Power and Energy Magazine, Jan.-Feb. 2012, V: 10 I:1, pp 49 - 57 , ISSN: 1540-7977,.

[47] Technische Richtlinie- BSI-TR-03109-1, Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, Bundesamt für Sicherheit in der Informationstechnik, ver.1, (Release Candidate), 21.12.2012.

[48] Mármol,F.G., Sorge,C., Ugus, O., Pérez,G.M., "Do Not Snoop My Habits: Preserving Privacy in the Smart Grid", IEEE Comm. Magazine, May 2012, pp 166-172

[49] Xia,J.; Wang Y.; "Secure Key Distribution for the Smart Grid" IEEE Transactions on Smart Grid, Vol. 3, n 3, September 2012.

[50] Framework Privacy by design. Canada. Available at: <http://www.privacybydesign.ca>, accessed on Nov 18th, 2012.

[51] Task Force Smart Grids Expert Group 2: "Regulatory Recommendations for Data Safety, Data Handling and Data Protection Report", February 16, 2011.

[52] van Blarkom, G.W.; Borking, J.J.; Olk, J.G.E. (2003). "PET". Handbook of Privacy and Privacy-Enhancing Technologies. (The Case of Intelligent Software Agents). ISBN 90-74087-33-7

[53] A. Rial and G. Danezis: Privacy-Preserving Smart Metering. TR, Microsoft Research, 2010

[54] C. Efthymiou and and G. Kalogridis: Smart Grid Privacy via Anonymization of Smart Metering Data. First IEEE Intern. Conference on Smart Grid Communications. IEEE, October, 4-6 2010

[55] F. D. Garcia and B. Jacobs: Privacy-Friendly Energy-Metering via Homomorphic Encryption. Security and Trust Management (STM 2010). Springer, 2010

[56] Petrlic, R.: A privacy-preserving concept for Smart Grids, 18. Workshop „Sicherheit in vernetzten Systemen“ (Sicherheit in vernetzten Systemen: 18. DFN Workshop), pp. B1-B14, Books on Demand GmbH, 2010.

[57] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-03109 Smart Energy. Version 1.0 (Release Candidate), 21.12.2012.

[58] Rede Inteligente. Abinee cria grupo de smart grid e trabalha na criação do Sibma. Available at: <http://www.redeinteligente.com/2011/01/20/abinee-cria-grupo-de-smart-grid-e-trabalha-na-criacao-do-sibma/>, accessed on Jul 11th, 2011.

[59] Hoenkamp, R. The Neglected Consumer the Case of the Smart Meter Rollout in The Netherlands. Available at SSRN 1917455, 2011.

[60] ANEEL: Res. normativa Nº 502. Available at: < http://www.aneel.gov.br/cedoc/ren2012502.pdf>, 07/08/2012.

[61] Lo,C.H; Ansari;N., The Progressive Smart Grid System from Both Power and Communications Aspects. IEEE Communications surveys & tutorials, vol. 14, no. 3, third quarter 2012 799.

[62] INMETRO. Portaria nº 375, Available at: <http://www.inmetro.gov.br/legislacao/rtac/pdf/RTAC001738.pdf>, September 2011.

[63] ANEEL. Resolução Normativa Nº414, Available: <http://www.aneel.gov.br/cedoc/ren2010414.pdf>. 09/09/2010.

[64] Ponemon Institute: Perceptions about Privacy on the Smart Grid. Research Report, Nov 2010.

[65] Interoperability - Review of Meter Protocols, NSMP Business Requirements Work Stream, December 2010, Martin Gill, KEMA Consulting

[66] M. Newborough, P. Augood: Demand-side management opportunities for the UK domestic sector. IEE Proc. of Generation Transmission and Distribution 146 (3), 1999, 283-293.

[67] A. Cavoukian, J. Polonetsky, C. Wolf (Information and Privacy Commissioner of Ontario, Canada, and The Future of Privacy Forum): Smart Privacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation. 2009.

[68] A. Cavoukian (Information and Privacy Commissioner of Ontario, Canada): Operationalizing Privacy by Design: The Ontario Smart Grid Case Study. 2011.