eEnergy

Trust and information security at a challenge

Trust and privacy in eEnergy Demand Response Program

TDL | Trust in Digital Life

Authors:
Gabriel Waller
Ionut Ventura

Table of Content

1. Introduction

The declining levels of natural resources and the increasing demand on energy consumption make the introduction of the Smart Grid (SG) essential. The smart grid optimizes energy usage, but also integrates the renewable and alternative energy sources. The impetus for alternative sources is even more evident now with the need to re-visit the safety of nuclear sources in the wake of recent catastrophic events in Japan.

The energy conservation reform must be a common effort of all the stakeholders. While implementing the smart grid is essential to build and realize its benefits, the complexity of this new innovative technology introduces new vulnerabilities and concerns about consumers' privacy protection. The smart grid greatly expands the amount of data that can be monitored, collected, aggregated and analyzed. For example, specific appliances and generators can be identified from the signatures they exhibit in electric information at the meter when collections occur with great frequency as opposed to through traditional monthly meter readings. This more detailed information expands the possibility of intruding in consumers' privacy expectations.

Martin Pollock from Siemens Energy said at the Smart Grid and Cleanpower conference in Cambridge: "We, Siemens, have the technology to record it (energy consumption) every minute, second, microsecond, more or less live. From that we can infer how many people are in the house, what they do, whether they're upstairs, downstairs, do you have a dog, when do you habitually get up, when did you get up this morning, when do you have a shower: masses of private data. We think the regulator needs to send a strong signal to say that the data belongs to consumers and consumers alone. We believe that's a blocker to people adopting the technology".[1]

Fortunately, the smart grid is at a nascent stage, so this is the moment to adopt the adequate privacy design, by understanding and respecting consumers' reasonable expectations of privacy, security, and control over who has access to potentially revealing energy-usage data. Only this way the trust of the consumers can be gained and they can be attracted to participate in. The lack of an adequate privacy design of the smart grid could lead to:

- loss of consumer trust
- hinder smart grid deployment efforts
- lower demand for new products
- reduction of innovation

The purpose of this paper is to trigger a challenge in identifying threats to privacy and in determining accurate and comprehensive privacy and trust principles, for the professionals involved in the smart grid technology development and deployment.

We aim to achieve this objective by elaborating an user scenario starting from the existing studies, from the practical experiences of the companies who are already installing and operating the smart grid (e.g.: in some cases, the utility's technicians have faced roadblocks as they tried to enter communities to install the equipment[2]) and from the principles and experiences from other business sectors like financing and telecommunication.

The user scenario provides an overview of identified threats and gives suggestions for future study. This use case scenarios will be used to provide input for the other Trust in Digital Life (TDL) working groups: WG2: Technology & Requirements, WG3: Law & Technology, WG4: Business Cases, and contributions to the Strategic Research Agenda of TDL.

[1] http://www.reuters.com/article/2010/06/25/us-energy-smart-idUSTRE65O1RQ20100625
[2] http://www.treehugger.com/files/2010/12/smart-meter-protest-blockades-road-forces-pge-trucks-to-retreat.php

2. Summary

The user scenario aims to find some answers to the possible consumers' questions, raised by the concerns on the privacy of the data that can be monitored, collected, processed and analyzed in the smart grid:

- What customer data is collected and why?
- Who owns the data?
- Who collects, stores and processes the consumers' data?
- Where the data are stored? What jurisdiction is applicable?
- What data is shared with other organizations?
- How long the data is stored?
- How accurate and reliable the data is for the intended purpose?
- What are the means to prevent unauthorized use of customer data?
- How can the customer check his/her data?
- What audit and verification procedures are in place to ensure customer trust and security?

In this purpose we develop a user scenario on Demand Response (DR) program choosing actors from the categories of stakeholders identified and listed in the table below:

Stakeholders	**Objectives**
Utilities	To monitor electricity usage and load; to determine bills
Consumers	To reduce bills; To protect the privacy of their personal data
Electricity usage advisory companies	To promote energy conservation and awareness
Third party companies	To develop energy usage management services for consumers
Insurance companies	To determine health care premiums based on unusual behaviors that might indicate illness
Marketers	To profile customers for targeted advertisements
Law enforcers	To identify suspicious or illegal activity
Civil litigators	To identify property boundaries and activities on premises
Landlords	To verify lease compliance
Private investigators	To monitor specific events
The press	To get information about public persons
Creditors	To determine behavior that might indicate creditworthiness
Criminals	To identify the best times for a burglary or to identify high-priced appliances to steal[3]
Malicious individuals	To determine behavior of the consumer for malicious purposes (e.g. revenge, information, blackmail, kidnapping)

3. Narratives

3.1. Privacy in Demand Response program

Demand response is the term used to identify a utility or a third party action to reduce or shift peak demand load through consumer incentives and direct load curtailment. The pricing models set peak/off-peak pricing tiers to provide consumers with an economic incentive to shift their energy consumption to off-peak hours. It is the consumer's choice based on existing incentive to shift the use of appliances to off-peak hours. The choices by the consumer might be made automatically using embedded control devices that manage consumption locally, according to variable tariff signals.

[3] NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid August 2010

Generally, in order to have high peak load reductions through tariffs and demand response, the building systems have to be automated to optimize their use in peak-load situations. These can be very effective and deliver the largest savings and peak load reductions; however the technology is still quite more expensive than the "one-meter per household" systems, in which case the utility pays for the investment. The home automation technology doesn't bring only a monetary costs, but also very important costs in terms of customers' privacy. Mitigating these privacy concerns is the subject of this use case.

3.2. Actors

Johanna B.	31 years old engineer, residential consumer, customer of X Utility Company
X Utility Company	Johanna's electricity utility company
Electricontrol Company	Third party demand response service provider

3.3. Context

Subject:
The trust and privacy aspects of the mechanisms by which Johanna, the utility's customer grants permission for the X Utility Company to share her data (such as meter usage data) with the Electricontrol Company, Third Party service provider, so that Electricontrol may provide the desired demand response service to Johanna.

Target group:
Residential customers (Small houses and apartment buildings)

The service:
Demand Response, energy savings and peak demand reduction through home automation.

Description of the service:
Both X Utility Company and a third party named Electricontrol Company develop and offer applications that control the home automation systems. In addition to the exact consumption information, the systems minimize energy consumption and benefits more from the dynamic tariffs by automatically using less electricity at peak times.
An important difference between the two demand response services provided is that the third party needs consumers and pricing data from the utility company.

Requirements:
At least automated meter reading (AMR), real-time connection and control to home automation

Consumer expectation:
Householders can expect to reduce their electricity consumption by tens of percent by combining smart meters with smart home automation in existing homes[4], depending on the nature of the technology used and the consumer's own consumption behavior. More specifically, the greatest savings, up to 33% are possible at peak consumption times, through the use of substantially higher 'critical-peak' pricing in combination with the use of home automation such as the use of home heating/cooling systems.

Assessment of the service:
The home automation system is still quite expensive and therefore not all the consumers can afford it.

[4] http://www.vaasaett.com/2010/06/respond2010launch/

3.4. User Scenario

X Utility Company monitors, collects and analyzes information such as home temperature and energy usage from the smart devices, smart meters, thermostats, and wireless sensors located at Johanna's residential site. The information is transmitted through internet. The data is processed by utility's own energy management and control application in order to reduce electricity demand as well as to provide a cost effective mechanism for flexible and reliable grid. Demand response sends signals via network to resident appliances and controls the energy usage. The exposure of the large amount of private data resulting from this process leads to Johanna's concern on privacy.

Concerned that possible attacks such as data manipulation attacks, masquerading, eavesdropping and repudiation can lead to false demand response event configuration and unauthorized access to her private information, Johanna decided to choose a third-party application as demand response service provider. She learned from advertising articles about a specific management and control application provided by Electricontrol Company, and decided to authorize that application, and no other, to have access to home appliances she is using and their usage pattern.

The access to the data on energy consumption generated by smart meters, owned by the X Utility Company and transmitted by the smart grid, is critical to enable Johanna and Electricontrol Company to perform the demand response program. As owner of the customer energy usage data (CEUD), Johanna submitted a request to X Utility Company to allow the Electricontrol Company to access her energy consumption data collected by the smart meter.

The third party can acquire consumption data needed for demand response program from three sources:

1) From a home area network (HAN) enabled device which obtains data from the smart meter and passes it on. Such a non-utility HAN-enabled device must be authorized in order to enable the direct transfer of data from the smart meter. The authorization process requires that the device is "registered" by the particular smart meter. The utility will provide this registration service pursuant to utility tariffs.

2) From the customer, who obtains the data from the utility or from the smart meter.

3) From the utility company. In this case, in our opinion, a contract is required between the X Utility Company and the third party, by which the latter is obliged to implement and maintain security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. The signed agreement should additionally prohibit the use of the data for a secondary commercial purpose without the consumer's consent.
   The utility must ensure equal regulatory treatment for all third parties who acquire usage data from the utility and those who acquire usage data from a device.

3.5. Ownership of consumer data

In the aim to find the best solution for Johanna's request it is essential to unanimously accept a decision on the division of roles and responsibilities regarding the ownership, the possession and the access to the customer data.

The ownership of the data remains still a debatable topic. Different viewpoints have been provided in this respect by varied entities involved in the demand response program. According to some opinions, either the customer owns the data or the utility. Some have stated that the data belongs to the customer, as the customer generates energy data by

updating the energy consumption based on the demand response event and revealing PII to the utility. Others refute to this by stating that the utility installs, executes and maintains the demand response program for cost effective energy usage. The demand response event initialized by the utility allows the consumer to update the electricity usage and thereby producing energy consumption data for billing and other operational functionalities carried out by utility. Others stated for a middle stand for the ownership of data between utility and customer. Since the customer generates data and the data is used by utility for operational purposes, they stated that data should be co-owned between the two. Consequently, clear concise information has not been met regarding the ownership of data.

The privacy and security laws vary widely from place to place. In the European Union the Privacy Directive 95/46 EC establishes a presumption that Personal identifiable information (PII) belongs to the data subject. Such information may be processed only for specified, legitimate, and limited purposes where there is either valid consent from the data subject or a legitimate need of the data processor that outweighs the data subject's general privacy interests. This general privacy right extends to PII collected by the smart meters. EU Member States will have to adapt the specific national legislation in full compliance with the EU and national data protection legislation.

In our scenario we assume that the customer is the energy usage data owner. The issues to access and control the data have the same importance as ownership of the data. The custodian of energy data, which can be the utility or an independent customer portal, should consider managing and safeguarding the information in accordance with the legal framework. Customers should have access to customer specific energy usage data (CEUD), and allow the utility and the third party to access it.

In the current user scenario:

- The Resource Owner is Johanna, the electric utility customer.
- The X Utility Company should fill the role of the Resource Custodian by managing the customer's electricity usage data.
- The Third Party Company Electricontrol enter the picture by providing Johanna Demand Response service that requires access to data from the custody of the customer's utility (such as meter usage data).

3.6. Resource Owner's permission for the Resource Custodian to share his/her data with the Third Party

The mechanisms by which Johanna, the Resource Owner, grants permission for X Utility Company, the Resource Custodian, to share her data (such as meter usage data) with Electricontrol Company so that the Third Party may provide the Demand Response service to Johanna is the subject of a relationship among the three parties:

A. Johanna interacts with X Utility Company to select the resource (e.g., usage data for a particular meter) for which she wishes to grant access to Electricontrol and any necessary attributes of the relationship (e.g., the period during which Electricontrol should have access to data).

   Step 1: Johanna requests that the X Utility establish a new data access relationship.

   Step 2: X Utility presents Johanna with a list of resources and any additional attributes (e.g., duration for which permission should be granted) that can be shared with Third Parties.

   Step 3: Johanna selects the resources to share, sets any available attributes for the relationship, and specifies the Third Party to the X Utility Company. Selecting these

parameters and completing the interaction indicates permission for X Utility to grant Electricontrol access to the specified shared resource.

Step 4: The relationship will only be created if X Utility accepts the selections for Electricontrol (e.g., a X Utility may constrain access to certain resource attributes depending on resource sensitivity).

Step 5: X Utility generates a Shared Resource Key for this relationship and provides it to Johanna. Each Shared Resource Key is unique to the relationship between Johanna, X Utility, and Electricontrol for a particular resource.

Step 6: X Utility notifies Johanna of the creation of the Shared Resource Key and establishment of the relationship. No acknowledgment or confirmation is required.

B. Johanna interacts with Electricontrol to establish the DR service relationship under a contract.

Step 7: Johanna requests that Electricontrol complete the establishment of the new data access relationship.

Step 8: Johanna provides the Shared Resource Key to Electricontrol.

Step 9: Electricontrol persists the Shared Resource Key, associating it with its relationship with Johanna.

C. X Utility provides Electricontrol with shared resource information (e.g., usage data) in accordance with the permission granted by Johanna.

In this process when X Utility provides Electricontrol with shared resource information (e.g., usage data) in accordance with the permission granted by Johanna, the following privacy recommendations should be respected:

1. X Utility shall not release PII to Electricontrol.
2. X Utility and Electricontrol shall not disclose any of Johanna's sensitive data to external parties without explicit authorization by Johanna.
3. Johanna requesting/granting access to data must be authenticated and authorized to manage privileges for that data.
4. Johanna shall always receive timely notification of changes in access to her sensitive data.
5. Only trusted Third Parties shall participate in the exchange of data.
6. Data must be exchanged in a secure way.
7. Johanna should have access to a simple interface (e.g., a web browser) to interact with X Utility and Electricontrol.

The third-party data access relationship shown in Figure 1 shows how this pattern could be applied in a setting in which the utility fills the role of the Resource Custodian and the demand response service provider fills the role of the Third Party.

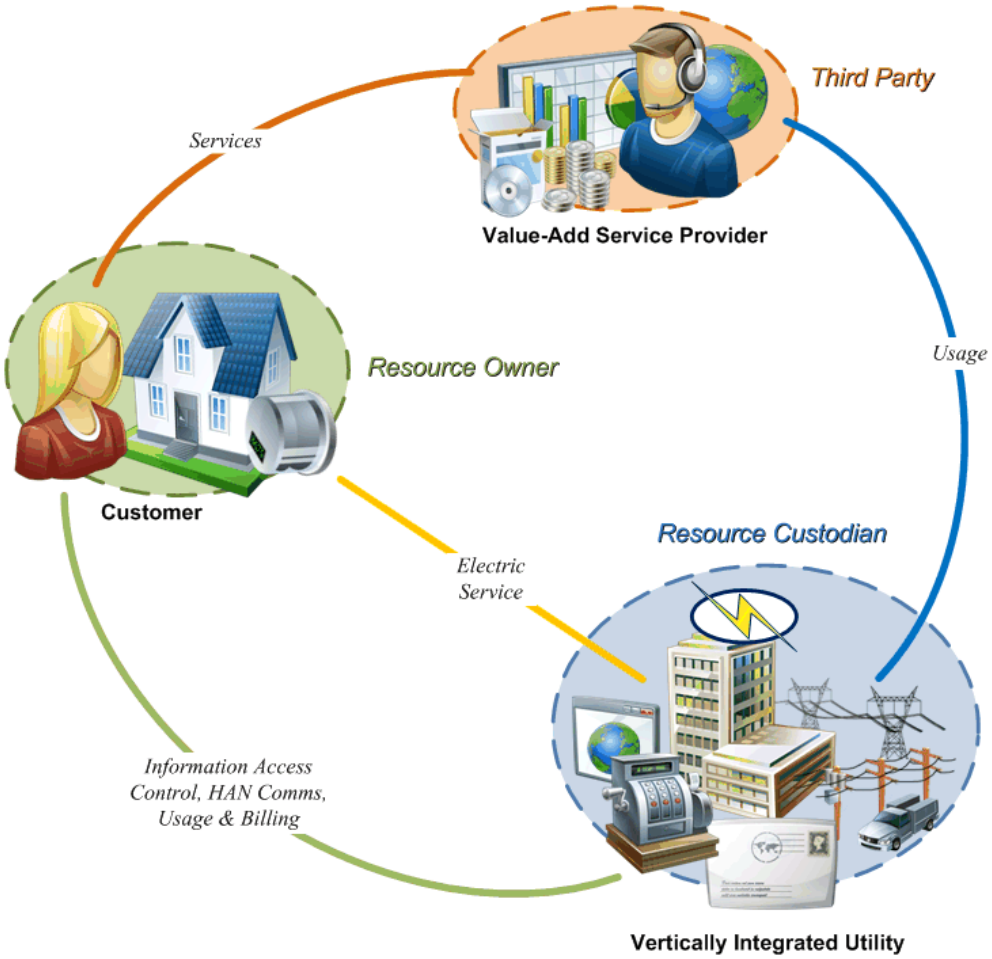

Figure 1: Data flow in demand response service, with utility filling the Resource Custodian role

The third-party data access relationship pattern could be applied also in a setting in which an independent customer portal (e.g., not run by a vertically-integrated utility) fills the role of the Resource Custodian and the demand response service fills the role of the Third Party, as shown in Figure 2:

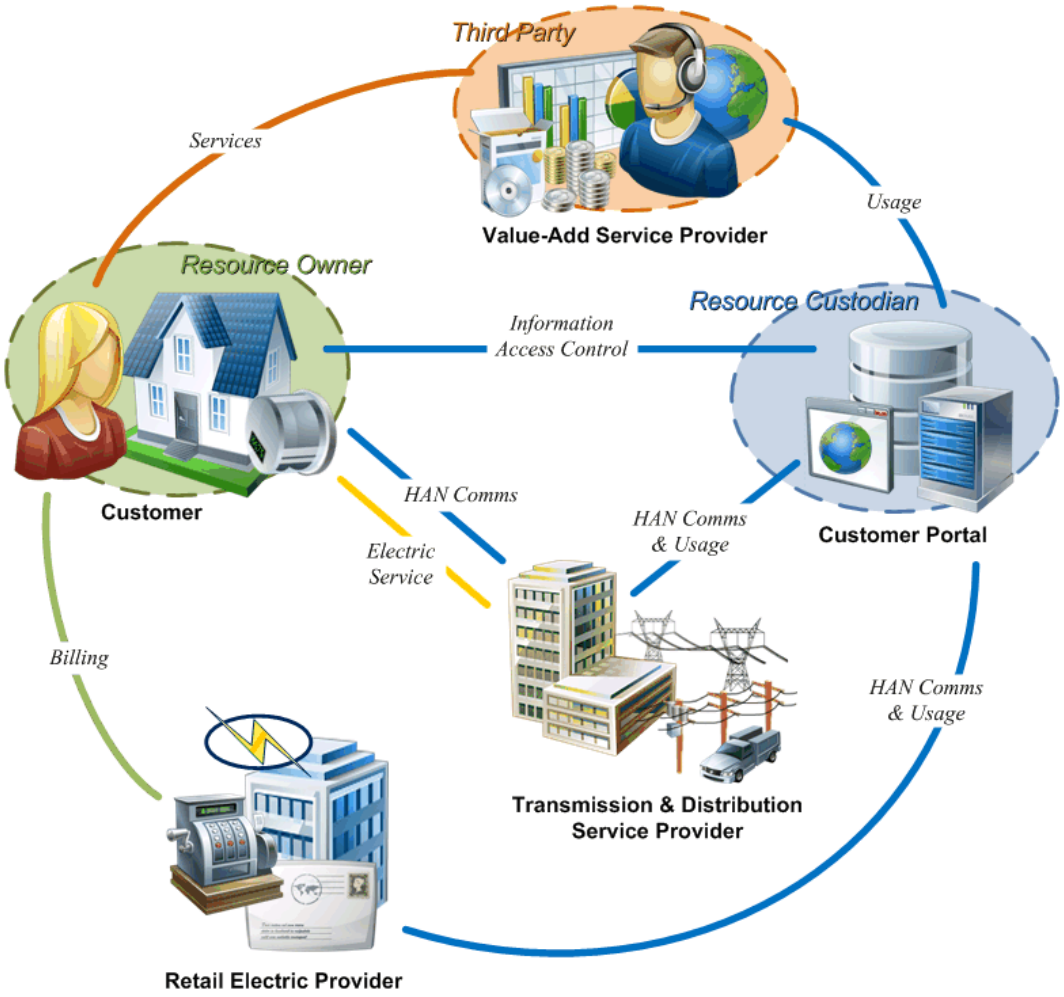

Figure 2: Data flow in demand response service, with independent customer portal filling the Resource Custodian role

3.7. The Resource Owner's extension or restriction of permissions for the Resource Custodian to share its data with the Third Party

In the event that Johanna would want to restrict or extend the permissions for the Resource Custodian to share its data with the Third Party, the following procedural steps should take place:

Step 1: Johanna chooses to modify relationship permissions with X Utility.

Step 2: X Utility presents Johanna with a list of resources that can be shared with Third Parties.

Step 3: Johanna chooses particular resource whose permissions she wishes to modify.

Step 4: X Utility provides available resource attributes and current settings to Johanna.

Step 5: Johanna chooses new settings.

Step 6: The new permissions governing the relationship will apply only if the X Utility accepts the selections for Electricontrol (e.g., X Utility may constrain access to certain resource attributes depending on resource sensitivity).

Step 7: X Utility will use the new permissions from this point forward to govern the relationship (until further changed or the relationship is terminated).

Step 8: X Utility notifies Electricontrol that permissions have changed (identifying the resource by its Shared Resource Key). No acknowledgement or confirmation is required.

Step 9: X Utility notifies Johanna that permissions have been changed. No acknowledgment or confirmation is required.

Step 10: Electricontrol handles any data not consistent with the new permissions in the manner specified in any service agreements among the parties in the relationship.

S11: Electricontrol will use the new permissions, associating them with the Shared Resource Key.

3.8. The termination of the relationship between the Resource Owner and the Third Party

In case Johanna would like to terminate the contractual relationship with Electricontrol the below procedure should be followed:

Step 1: Johanna requests that X Utility terminate the data access relationship.

Step 2: X Utility presents Johanna with a list of resources for which there are valid relationships with Third Parties.

Step 3: Johanna chooses the resources whose relationship is to be terminated.

Step 4: X Utility terminates the relationship, deleting the appropriate Shared Resource Key from its list of valid relationships.

Step 5: X Utility notifies Electricontrol that the relationship has been terminated (identifying the relationship by its Shared Resource Key). No acknowledgement or confirmation is required.

Step 6: X Utility notifies Johanna that the relationship has been terminated. No acknowledgment or confirmation is required.

Step 7: Electricontrol handles any data not allowed by the termination of the relationship, in the manner specified in any service agreements among the parties in the relationship.

3.9. Privacy impact assessment

The privacy impact assessment (PIA) represents a structured type of analysis, repeatable, whose main purpose is to identify the risks and effects of unwanted events that might occur in the process of collection, maintenance, and dissemination of PII in Demand Response program.

The PIA process, by its nature, is meant to be best completed it at this stage when it can change the development of projects in a efficient and cost effectively manner. A PIA needs to be differentiated from a privacy or data protection audit. An audit is initiated on a project that has already been implemented. An audit proves its value if it either confirms that privacy undertakings and/ or privacy laws are being complied with, or if it highlights issues that need to be addressed.

The following table describes a model of PIA that Electricontrol Company could perform in order to develop processes and practices mitigating privacy risks:

Event	Type of data	Threat	Impact
Demand response service provider configures the demand response program and initiates the event in Demand Response Automation Server (DRAS)	Program type, date & time of the event, geographic location, customer list	Eavesdropping on this information is not concerned since the information may not be regularly sent, but the information needs to be protected	Medium on confidentiality
		Unauthorized manipulation on this information could affect the demand response program behavior. For example, an attacker can change the demand response program's geographic location and thus affecting a wrong customer site	Medium on integrity
		Failure in communication between utility and the third party because of interception of data by an unauthorized party	Low on availability
Utility initiates the bid request to DRAS	Program type, date and time of the event, date & time issued, geographic location, customer list, request for a bid	Eavesdropping on this formation could result in the leak of bidding information	High on confidentiality
		Unauthorized manipulation on	High on integrity

	(RFB) issue date and time, RFB close time, price offered for load reduction per time block	this information could affect the bidding program behavior	
		Failure in communication between utility and the third party because of interception of bidding data by an unauthorized entity	Low on availability
The Utility Program Notifier gets the updated demand response event information from the utility information system (UIS) and initiates the event in DRAS.	Participant list, accept or reject information	Eavesdropping on this formation could invade the privacy of the participant	High on confidentiality
		Unauthorized manipulation on this information could affect the demand response program behavior, such as modification of account numbers, accept or reject bids and customer list for the demand response program	High on integrity
		Failure in communication between utility and the third party because of interception of data by an unauthorized party	Low on availability
Demand response event information sent to the DRAS client at the participant site to modify the energy usage in the demand response program	Demand response event information such as date and time of the event, date and time issued mode and pending signals is sent to the demand response client	Eavesdropping can cause invasion of customer privacy	High on confidentiality
		Unauthorized manipulation on this information could have financial impacts on customers and affect the stability of the grid. The source needs to be authenticated and authorized before sending the signals	High on integrity
		Failure in communication between the	Low on availability

		demand response service provider and participant sites.	
Information sent to the notifier consisting of acceptance or rejection notification to the participant or facility manager or aggregator	This information is provided through email, phone call or page	An adversary may manually send an email, make a phone call or submit a page to the participant or facility manager so that the manager may respond to the adversary instead of to the demand response service provider or the manager may take a wrong action in response to the notification	Low on integrity
DRAS client located at the participant site sends the load status information to DRAS	Program identifier, facility or participant identifier, date and time of the event, shed data in kW/kWh, load reduction end uses (HVAC, lighting.), event type (Day-Ahead or Day-of)	Eavesdropping on this formation could invade the customer privacy	High on confidentiality
		Unauthorized manipulation on this information could make DRAS not be able to record the actual response to the demand response events received of the DRAS client. The DRAS may make an inappropriate response to the demand response program corresponding to the false system load status	High on integrity
		Failure in communication between DRAS and DRAS client	Low on availability

3.10. Privacy concerns

Based on the PIA performed findings, Electricontrol Company could gain Johanna's trust by developing and advertising detailed privacy policies that should address the following identified privacy concerns:

A. **Identity theft.** Personal identifiable information (PII) (social security number, address, date of birth, driver license, email address, IP address, logs records and passwords of the customer) stored at the third party will be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure.

B. **Determine personal behavior patterns.** Patterns associated with number of people living in the house, use of electrical appliances, and absence of residents can be determined through smart devices monitoring techniques. Even supposing that the data is kept anonymous, several combinations of each data item of PII could expose an individual's information. For example, studies revealed that combinations of date of birth and geographical location could predict social security number (SSN) of an individual. PII information such as customer name, address, meter location and meter ID combined would divulge electricity load information pertaining to geographical location, electricity usage, customer behavior patterns and devices used at residential site. The third party will guarantee protection against leakage of information associated with the house through smart meter and avoid unauthorized determination of personal behavior.

C. **Determine specific appliances used.** Smart devices such as smart meter, thermostats, and sensor networks at residential place can track the use of specific appliances like washing machine, refrigerator, television, heater, and air conditioner. An incoming demand response event could be to switch off the air conditioner during peak time. This information will be protected from possible attackers who could use, for example, the tracking of the alarm systems to operate a home invasion.

D. **Determine personal behavior patterns of tenant by owner of residential site.** Property owners at the residential site will have access to the smart meter and thus will be able to identify personal behavior patterns as well as home devices belonging to the tenants which may raise privacy concerns if consent from tenant is not obtained. The third party will allow the owner to access the data collected from the smart meter related to the tenant's electricity consumption, but will not share the detailed information on the track of use of specific appliances that could determine the personal behavior of the tenant without tenant's consent.

E. **Mismanagement of data storage and processing.** Information such as energy data from the smart devices, customer registration with the demand response program, bidding price information, and utility administrative data is stored, accessed, modified and processed. The data is complied based on electric market prices after which demand response signals are routed to other subsystems of smart grid. Information might also require some data preprocessing and data mining techniques for billing, real time information for customer support/technician as well as for predicting the future values. Privacy concerns include questions regarding the type of data to be collected, which places it will be routed and where and how will it be stored. If proper access control mechanisms are not maintained then an adversary within the operator and its sub-systems can process incorrect and route data to a different entity. The third party will secure the storage and processing of the customer data in order to avoid disclosure to the unauthorized parties that can lead to privacy impact associated with the customer lifestyle pattern and to identity theft. Information collected from the residential site will be secured and limited to the extent that resolves the purpose of demand response program.

F. **Internal management, training programs and audits.** Organizations that access or provide data to the smart grid should appoint personnel to a position responsible for ensuring that documented information security and privacy policies and practices exist and are followed. Information security and personal information privacy practices should include requirements for regular training and ongoing awareness activities. Audit functions should also be present to monitor the smart grid data access activities. Electricontrol has documented information security and privacy responsibilities and authority within the organization. The company will regularly perform information security and privacy training and awareness programs and will monitor access to smart grid data.

G. **Information sharing with other parties.** The real-time data streaming capabilities of the smart grid may be very attractive to large appliance manufacturers, marketers interested in usage information on utility or non-utility dependent small appliances, devices, or other consumer products.[5] The smart device information will not be provided to other parties without customer's consent and only under written agreement. The contract will specify that the third party must implement and maintain security procedures and practices appropriate to the nature of the data, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Proper secure mechanisms will restrict the third party to carry out marketing practices through information obtained from devices and private customer information. The customer will be always notified regarding the type of information, purpose for which and destination where the information is routed.

H. **Customers' access to their Personal Identifiable Information (PII).** The smart grid has the capability to facilitate the interaction of the users with their electricity usage information through modern means, such as Internet, mobile phones and personal digital devices. Therefore, the transmission or publication of smart grid data via Internet raises privacy challenges. Internet communications are generally unsecure. In essence, the access to the smart grid data over the Internet creates risks similar to those when accessing any other type of personal information over the Internet.. Electricontrol will protect the content against unauthorized interception, manipulation, or other compromises when publishing the information. Moreover, users do not always have complete knowledge of, or control over, how their data will be used. There might be times where customers are unaware of their own private information laid out to the utility and other organization. The customers will be allowed to make changes to any inaccuracies related to their PII. The third party proposes various secured solutions for customers to access their PII. Consumers will also be given some control over the demand response features and will receive assistance in order to make better decisions regarding the consumption of electricity.

I. **Notification for the PII new information use purposes and collection.** Whenever new collection, use, retention and sharing of energy data and PII are needed, a clearly specified notice should exist and be shared in advance. Electricontrol will notify the consumer also before starting to use existing collected data for materially different purposes other than those the consumer has previously authorized. In addition, Electricontrol will notify the recipients of services before they will start collecting additional data beyond that already being collected, along with providing a clear explanation for why the additional data is necessary.

J. **Breach notice practice.** Electricontrol will set up policies and procedures to identify breaches and misuse of smart grid data, along with expanding or establishing procedures and plans for notifying the affected individuals in a timely manner with the

[5] Elias Leake Quinn, *Privacy and the New Energy Infrastructure* 28 (2009), *available at* http://ssrn.com/abstract=1370731

appropriate details about the breach. This is particularly important with the transmissions of billing information from the utility in the smart grid environment.

K. **Commissioning, registration and enrollment of home area network (HAN) devices.** A home area network is created by the smart devices through a process called commissioning in which each authenticated device joins the network and exchanges information such as network key, device ID, device type and receives broadcasted signals. Each device is able to join the network through an installer and based on the manufacturer's instructions. Each smart device registers itself with other devices within the home area network through mutual authentication process. The customer then enrolls itself with demand response program so that the demand response service provider can communicate with smart devices. The third party will secure the access controls in order to restrict the third party installers and maintenance personnel to determine customer's private information. In addition, customer and home device information provided to third party during registration will be properly secured to avoid privacy issues. Home devices communicating through wired networks will be protected against attacks from rogue devices that eavesdrop the communication or tamper the device.

L. **Compliance with the legal and regulatory framework of demand response.** Developing legal and regulatory regimes that respect consumer privacy in cooperation with the data protection authorities, in particular with the European Data Protection Supervisor, is fundamental for the large acceptance of demand response services by consumers. Facilitating the consumers' access to their energy data processed by third parties and ensuring their control over it is also crucial. If the data processed is technical and does not relate to an identified or identifiable natural person, then the third party could process such data without needing to seek prior consent from grid users. The demand response service provider will always notify national data protection authorities of the processing of personal data and will assure the compliance with the principles and the provisions of the legal and regulatory framework.

4. Conclusion and further study

4.1. Privacy principles

Based on the identified privacy concerns, the international generally accepted privacy principles and the existing utility policies for the privacy protection of customer information, along with consideration of safeguards as found in the international information security standard ISO/IEC 27001[6], the proper privacy principles applicable to smart grid can be developed:

1. **Management & Accountability**: Organizations must formally assign staff with privacy responsibilities and make sure that privacy policies and practices exist and are followed. In the same time, regular training of the employees who use PII and are auditing the use of PII to determine compliance with the privacy principles and other applicable privacy protection requirements are a must.

2. **Notice & Purpose**: Consumers must be notified of the collection, use, retention, and sharing of PII before collecting the data.

3. **Choice & Consent**: Consumers should be presented with options on how any PII collected from them may be used, specifically for secondary uses of information

[6] International standard ISO/IEC 27000, First edition 2009-05-01, Information technology — Security techniques — Information security management systems — Overview and vocabulary

beyond those necessary for utility operations. The choice must be simple to make. The organization must also obtain explicit consent or implicit consent, when this is not feasible, with respect to the collection, use and disclosure of their PII.

4. **Collection & Scope**: The collection of data should comply with the law and should be limited to PII that is required to fulfill the stated purpose. Information must be collected directly from each individual person unless there are very good reasons why this is not possible.

5. **Use & Retention**: Information should only be used for the purpose for which it was collected. PII should only be kept as long as it is necessary to accomplish the purposes for which it was collected.

6. **Data minimization and anonymization.** Only PII needed to accomplish identified purposes should be collected. PII should be aggregated or anonymized wherever possible to limit the potential for computer matching of records.

7. **Individual Access**: Organizations should provide a process for PII data subjects to allow them to access, update and correct their own data.

8. **Disclosure**: PII should not be disclosed to any other parties except for those with the explicit consent of the individual or under authority of law.

9. **Security and Safeguards**: The organizations must protect the PII from loss, theft and must prevent unauthorized access, disclosure, copying, use, modification or destruction through the use of reasonable safeguards.

10. **Accuracy & Quality**: The organization must ensure that the PII is accurate, complete, timely and relevant for the purposes identified in the notice and that it remains accurate throughout the life of the PII within the control of the organization.

11. **Openness, Monitoring & Challenging Compliance**: The organizations must inform the privacy policies to consumers in a transparent way. The data subjects must be given the ability and process to challenge an organization's compliance with their privacy policies as well as their actual privacy practices.

4.2. Privacy best practices

The service providers in smart grid technology can substantially reduce the data privacy and security risks inherent by developing and adopting privacy best practices, by complying with the adopted privacy principles, the legal and regulatory framework, such as:

- Involve both technical and legal experts to resolve privacy and security issues at the system design stage. Only having a comprehensive approach, the developers can meet the technical, legal and ethical requirements and expectations.

- Collect only the data needed for specified purposes. The new smart meters and their coming along potential create the need for the data custodians to be more transparent and clearly give notice documenting the types of information items collected, and the purposes for collecting the data. Within the Smart Grid implementation there must be a clearly specified notice describing the purpose for the collection, use, retention, and sharing of PII.

- Retain the data only for the period of time related to the purpose for which they were collected. One purpose mentioned quite frequently is that the data collected from a meter would allow for the provision of energy efficiency advice, including year on year

comparisons. Such a long retention interval would only be adequate if the data subject has consented that he/she would take advantage of such a scheme.

- Provide consumers with meaningful, clear, and full notice prior to the collection, use, retention, or sharing of energy usage, data and personal information. The notice should feed a detailed description of all purposes for which consumer data will be used, including any purposes for which affiliates and third parties will use the data. The notice should also include how long the data will be maintained by the organization and which third parties the data will be shared with.

- Aggregate or anonymize personal information wherever possible to limit the potential for revealing private information. Smart Grid data should be aggregated in such a way that personal information or activities cannot be determined or anonymized wherever possible to limit the potential for computer matching of records.

- Implement privacy and security policies for internal and external access to PII. Data controllers must respect the rights of data subjects and must ensure that data subjects are able to exercise their rights easily using tools that enable their direct access to data.

- Define the data collection and use rights of customers, vendors, etc. in clear contractual language with strong privacy and security commitments and accountability for breach.

- Perform privacy impact assessment (PIA) for determining the privacy, confidentiality, and security risks associated with the collection, use, and disclosure of personal information (as described in the Section 3.9).

- Avoid resistance by permitting consumers to turn off or limit detailed data collection, especially during early research phases. Use the “privacy by default” principle when installing the smart metering equipment that means to make “Off” the default mode for data transmissions. For example, if the customer has a simple contract in which he pays the same price for electricity throughout the day, the meter will collect a daily single reading. Alternatively, if the customer has a contract for which there are different prices depending on the time of day, the meter will be collecting ten different readings every day. At its most basic level, Privacy By Default would ensure that meter readings are only transmitted as frequently as necessary for the operation of the system or the provision of a service the consumer has agreed to receive. This model could be adjusted in order to collect and store the load graph only on request.

- Consider privacy needs before the development of systems and processes by adopting privacy by design principles throughout the smart metering regulatory regime. A „privacy by design” approach ensures that privacy issues are identified at the earliest stages and recognizes the confidentiality issues that may arise. Privacy by design principles should apply to both domestic and non-domestic consumers.

- Train all utility and third party employees on how to access and on how to control the AMI data. Privacy protection requires more than enabling technology to protect data files stored on a server or transmitted between trusted partners, and more than privacy policies, periodic assessment tests, or appointing privacy and compliance personnel. A grassroots approach that provides employees with adequate training to correctly handle sensitive information is necessary.

- Perform internal and external audits. A privacy audit will assure that the company’s goals and promises of privacy and confidentiality are supported by its practices, thereby protecting confidential information from abuse and the company from liability and public relations problems. The audit ensures that information processing procedures meet privacy requirements by examining how CEUD is collected, stored,

shared, used and destroyed. The audit process needs to be capable of dealing with the full extent of the information system.
The audit process starts with the evaluation of the company's existing policies and procedures for legality and consistency with the company's mission and image. When policies have been reviewed, the data collected must be categorized according to the degree of security necessary. The audit assesses the sensitivity, security risks, and public perceptions of the information the company collects. The audit examines the necessity for each type of data, how it is collected, and what notice and options are provided to the individuals identified by the information. Mapping how data flows through the company for access, storage, and disposal can reveal privacy and security needs. The audit process itself must be conducted in such way to not increase risks and its recommendations must be addressed quickly once risks are identified.

- Establish incident response and breach notification procedures. An incident is a threat or event that compromises, damages, or causes a loss of confidential or protected information. Examples include unauthorized or accidental disclosure of information. All individuals' granted access to consumers' information or systems must be covered by the privacy policy and shall comply with associated procedures and guidelines. These individuals must include full and part-time employees, volunteers, contractors, temporary workers and others authorized to access information, network and/or systems. The guidelines must cover the incident reporting, analyzing, responding to, remediating, and documenting privacy and information security breaches.

- Establish Board of Directors and senior management to supervise the data privacy and the security practices and formally appoint positions and/or personnel to ensure that information security and privacy policies and practices exist and are followed.

- Educate the public about the privacy risks within the smart grid and what they as consumers can do to mitigate them. Both the public and private organizations involved in smart grid development must contribute to educate and inform consumers about smart grid's privacy issues. Consumers want to harness all the benefits of the smart grid, but in the same time to keep their privacy and safety intact. New educational campaigns should provide consumers with the information on how the smart grid can affect their privacy and on what stands in their power to protect themselves in this respect.
- Share information concerning solutions to common privacy-related problems. There is much diversity in the position across EU Member States, both in terms of progress of the implementation and energy supply arrangements, and the harmonization is highly needed.

- Implement standards, laws and regulations. There are various layers of action between EU Member States and different EU institutions that are currently working on standardization, regulatory recommendations and technical functionalities.

More research on layout regulations for third parties to handle load control devices, data storage, manufacturing smart devices, internet provision and application interfaces is required to adapt or extend this list.

4.3. Developing and adapting the legal and regulatory framework in the EU space

Due to the regulatory push by the European Union's Third Energy Market Package, most EU Member States have implemented or are about to implement some form of legal framework for the installation of smart meters. Moreover, in some Member States electronic meters with bidirectional communication are installed for economic reasons even without any specific legal requirements, but data privacy concerns are often raised and many network operators are still temporizing until there are official regulations and comprehensive laws for this topic.

The development of legislation and regulation for smart metering in Europe is highly dynamic due to the regulatory push and the efforts of market players. The provisions of national sectoral legislation that might apply should adapt to take into account the data protection specificities of smart grid. This is particularly important because the advantages of smart metering will come, not only with monetary costs, but also with costs in terms of customers' privacy. New privacy concerns will be born in the public discussions and will lead to new amendments of the laws.

Dutch Parliament adopted legal framework for voluntary installation of smart metering in November 2010 as a result of public debates on privacy. Most crucial in the debate was the publication of a report by university of Tilburg researchers, commissioned by the Netherlands' main consumer organization, to look into the privacy aspects of the smart meters. The report indicated serious privacy issues related to hourly and 15-minutes readings. This information could give away sensitive information about the consumer's habits (i.e. when someone leaves the house or returns). Second, the smart meter could provide insights into a family's living patterns and relationships "which can affect people's freedom to do as they please in the confines of their homes". Third, there is a risk that information about a person's energy use will fall into the hands of third parties such as the police or insurance companies. As a consequence, a mandated roll out of the smart meter is being considered a violation of the right to privacy as guaranteed by Article 8 of the European Convention on Human Rights.

The actual Dutch legal framework does not allow enforcement measures for the acceptance of the smart meter. The role of the government is to focus on stimulation, information and persuasion of smart meter acceptance. Areas for attention with respect to policy targets are the acceptance of the smart meter, the effective use of the smart meter and an efficient rollout of the smart meter.

The review of the EU data protection framework and the rules related to privacy is essential to clarify smart grid's privacy concerns. EU data retention requirements at Member State level should be harmonized to provide clarity as to whom the directive applies and allow for a single, coherent and cost effective retention period within the single market. In the case of data storage and processing outside of European space, the international dimension of data transfers in smart grid requires that operators be able to transfer data on a worldwide basis subject to appropriate safeguards for the processing of the data. In order to reduce the bureaucracy and burden on operators, harmonizing the notification and approval requirements mechanisms is required.

European policymakers should pursue on bilateral or multilateral international cooperation with regard to minimum protection levels for the privacy and security of data collecting, storage, processing and transferring. Smart grid's operators could face conflicting laws within and outside the EU, concerning disclosure of the information. Achieving a better understanding of jurisdictional issues and clarifying the definition of "personal data" across the single market is critical.

The ICT communities have to continue the development of technical standards for smart grid following the "privacy by design" approach and assess the network and information security and resilience of smart grid as well as support related international cooperation.

References

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

DIRECTIVE 2009/72/EC of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC

DIRECTIVE 2009/73/EC of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC

DIRECTIVE 2006/32/EC of 5 April 2006 on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC

DIRECTIVE 2010/31/EU of 19 May 2010 on the energy performance of buildings

NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid August 2010

International standard ISO/IEC 27000, First edition 2009-05-01, Information technology — Security techniques — Information security management systems — Overview and vocabulary

Draft Decision adopting rules to protect the privacy and security of the electricity usage data of the customers of PG&E, S.C.E., and San Diego G&E, 5/6/2011, proposed Decision before The Public Utilities Commission of the State of California

http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/Generally%20Accepted%20Privacy%20Principles.aspx

"Automation of Capacity Bidding with an Aggregator using Open Automated Demand Response", Lawrence Berkeley National Laboratory Demand Response Research Center. Available at: http://drrc.lbl.gov/pubs/cec-500-2008-059.pdf

"Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid," Information & Privacy Commissioner of Ontario, Hydro One and Toronto Hydro Corporation, June 2010, Available at: http://www.privacybydesign.ca/content/uploads /2010/03/achieve-goldstnd.pdf

"Security Profile for Third Party Data Access," The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG), January 2010. Available at: http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/DocumentsforReviewandComment/3PDA_Security_Profile_-_v0_20_-_20100129.pdf

"Data access and privacy issues related to smart grid technologies," Department of Energy. Available at: http://www.gc.energy.gov/documents/Broadband_Report_Data_Privacy_10_5.pdf

A. Cavoukian, Information and Privacy Commissioner, "Smart Privacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation," November 2009. Available at: http://www.ipc.on.ca/images/Resources/pbd-smartpriv-smartgrid.pdf

R. Herold, C. Veltsos, W. Pyles, " NIST Smart Grid High Level Consumer-to-Utility Privacy Impact Assessment *DRAFT* v3.0," NIST, September 2009.

Abbreviations

AMI	Advanced Metering Infrastructure
AMR	Automated Meter Reading
CEUD	Customer Energy Usage Data
CIA	Confidentiality, Integrity, and Availability
DR	Demand Response
DRAS	Demand Response Automation Server
HAN	Home Area Network
PIA	Privacy Impact Assessment
PII	Personal identifiable information
RFB	Request for a bid
SG	Smart Grid
SP	Service Provider
SSN	Social Security Number
TOU	Time-of-use
UIS	Utility Information System