

Smart Grid and the Home

Author: Guy Huntington, President, Huntington Ventures Ltd.

Date: August 16, 2010

Note: The views expressed herein are the author's own personal opinions.

Smart Grid and the Home – Privacy, Authentication and Authorization

Executive Summary

This paper outlines my own personal views on the requirements for the home customer re privacy, authentication and authorization. It's meant to illustrate the complexities and to raise questions in utility management, public regulators and utility customer minds about how customer privacy, authentication and authorization will be accomplished.

Privacy

Types of Data

In the future there are several types of utility customer data that privacy is applicable to:

- Customer account information – e.g. address, credit card information, billing information
- Customer account energy consumption – e.g. hourly, daily, weekly, monthly and yearly total home energy consumption information
- Home energy consumption – e.g. appliances, gadgets, air conditioners, heaters, lights, etc.
- Electric vehicle consumption

Parties Involved

There are several parties who may want to access such information including:

- Account owner – e.g. the home owner who is paying the bills
- Utility company
- Energy brokers
- Delegated identities – e.g. a caregiver for an elderly person or family members
- Other third parties – e.g. Electric car manufacturers, energy companies, battery manufacturers, hot water and air conditioning vendors, lighting vendors, etc.

Good and Bad

Smart grid means that the data becomes:

- “atomized” - i.e. more fine grained (second and hourly data)
- “personalized” - able to tell more exactly what goes on in every room in the home
- Commercially valuable to other parties than just the customer and the utility – e.g. energy brokers, hot water and air conditioning vendors, vehicle energy companies, etc.

From the home owner's perspective, this is good and potentially bad. It's good because the home owner can take advantage of a number of new services from the utility and other parties that will potentially lower their energy bills and manage their home energy.

It's potentially bad because the lifestyle of the homeowner can be deduced from the more atomic and personalized data. Further, this data can be quickly moved around to third parties, government agencies, etc without the home owner knowing about it and giving their consent.

Data Storage

The data itself may be stored on a temporary or permanent basis in the following locations:

- Home
 - Energy controllers of the future
 - Home area network
 - Home data stores
- Utility
 - Operational data stores
 - Data warehouses
 - Customer billing applications
 - Customer relationship marketing systems
 - Customer portals
 - Other applications in SCADA and Corporate
- Third Parties
 - Energy brokers
 - Etc.
- Government agencies
 - Police
 - Security agencies

Data Movement

The data also has movement. For example, the home data may go from the home to the utility to an energy broker and potentially beyond.

Data Expiry

Finally, the data also has potential expiry dates associated with it. For example, the home account owner may grant a third party or utility access to a particular piece or set of data for limited time duration only.

Implications

The implications of the above are significant for each of the parties:

Home Account Owner

With the Utility

The home account owner will want to ensure that their permission is given for the utility to:

- Use their customer account, account energy and home energy data internally or not approve the use of the data
- Approve the use by the utility of sharing or releasing any data with any third party
- Approve any delegated access to their account, account energy or home energy data
- Specify the time limit of the data that will be stored within the utility or shared by the utility with any third party

With Third Parties

The home account owner will want to ensure that their permission is given for the third party to:

- To approve the use of their data with third parties as well as specifying the time limit of the data

Utility

The utility:

- Must ensure that there is a fine grained control of data content with appropriate controls to ensure who can view the data regardless of where it is stored in the different utility applications and data stores
- Design the systems such that permission is given by the customer before the utility shares the data with third parties
- Be able to terminate access to data based on time limits the customer sets
- Have some kind of chain of custody of data such that if any litigation occurs the utility can prove that they protected the data appropriately within their enterprise and how they passed the data to third parties

Third Parties

Third parties will:

- Ensure that there is a fine grained control of data content with appropriate controls to ensure who can view the data regardless of where it is stored in the their customer applications and data stores
- Ensure that customer permission is given before taking in customer data
- Be able to terminate access to data based on time limits the customer sets

Technological Requirements

The privacy technological requirements for all the above are having good identity management, fine grained content management and digital privacy rights infrastructure in place by the utility and third parties. I also believe that the best way to handle the content is to have XML schemas that the utility and third party industry agrees to, defining each data element. This way the data that is being passed around can be easily interpreted by different applications regardless of how they store and label the content internally. It will also aid content management and privacy rights applications in the future apply and enforce security policies for data that is coming from another party.

For customers, it means that if they have their own energy data stores within their home, they need to grant access to the data to specified parties and be able to specify time limits on the data once it's left their data stores.

Authentication and Authorization

Assuming the privacy infrastructure is in place, let's now discuss the authentication and authorization requirements to the home. Many utilities are currently deploying smart meters in the homes. One of the main drivers of this is time of use billing being implemented resulting in customer bills that are climbing. Customers are not happy with this. As a result, many utilities are currently buying and deploying customer portals that offer their customers the ability to manage their home energy consumption as a way to lower their total monthly bill.

One of the unsaid effects of deploying this software is that the utility's applications need to talk to the home on a frequent basis whenever any "energy event" in the home occurs. This could be every few minutes or a longer period of time.

Most of the current deployments set a uid (uniform identification) and password in place allowing the application to log on to the local data store in the home. I believe that this approach is not secure from the customer's perspective since passwords are easily obtainable through a variety of different methods. I also believe that over the next several years, privacy litigation against utilities will force the utility to adopt a more rigorous method of authenticating to the home.

I think that the answer is to deploy web services to the home using a digital certificate that the home owner grants the utility as well as the utility granting a digital certificate to the home owner. These "tokens" provide a higher strength of authentication to automated or semi-automated interactions between the home owner's applications and data stores and the utility's applications.

There is a hidden cost in deploying a public key infrastructure (PKI) to achieve this. The utility must now manage digital certificates. This means that certificates must be issued, revoked and renewed. The utility will also use PKI to interface with third parties for authentication who are accessing the customer data via the utility since many of these interactions will be done via a web service automatically in the future.

Further, the average home owner won't know what these digital certificate tokens are. I predict that enterprises like Cisco, who own companies like Linksys, providing wireless routers to the home, will become the main technological interface to the home energy controller in the future.

The wireless router software will integrate with the home portal management software. The software will ask the customer if they wish to grant the utility access to their data. When the customer responds affirmatively, the software will generate a home digital certificate and grant this to the utility. Further, the router software will then generate a new digital certificate with the customer's permission when the digital certificate expires. This then removes the customer's potential confusion over digital certificate management. Finally the router will take the utility's digital certificate and store it securely on the router.

Now let's consider the customer logging on to the utility customer billing and portal applications to set who in their family has rights to change smart grid program settings with the utility, etc. There is significant customer ease of use considerations to consider.

First the utility must be able to offer different access rights to different home members. The utility's application software must be able to offer fine grained authorization rights to different family members allowing this to happen. Secondly, the utility must also have a way to accept delegation of account management and data access to the customer. For example, this will enable elderly customers to delegate the management of their accounts as well as offer different smart grid home energy settings to other family members.

This is good and potentially bad for a utility. In offering more services to their customers, there is now the need to grant authentication and authorization rights for many different parties than they do today. Using uids and passwords will not work with larger utilities since many people forget their passwords and there is an associated password management cost.

A better way for the utility to manage this mid-term is to use voice authentication to log on to the utility systems. The home owner would use their voice and wouldn't have to remember their uid and password to log on. It also easily enables different family members to log on using their voice and then have the utility's identity management infrastructure apply different authorization rights to the party.

One thing the utility might consider is for any changes to the home owner account settings, where the risk is higher to the customer and the utility, the customer might be required to also provide a password in addition to their voice. However, for regular home energy management functions, where the risk is lower, voice authentication is sufficient.

Summary

There are many hidden management costs in deploying smart grid services to the home. I believe that future litigation and regulation will force the utilities to deploy an extensive identity management, content management, privacy rights and public key infrastructure (PKI). Voice authentication should be offered as part of an identity management deployment.

If you agree with me, then now is the time to begin laying in place the budgets, project teams and infrastructure while most utilities are in the smart grid planning stages. This infrastructure normally takes one to three years to properly plan, deploy and maintain. Further, it is more complicated than it sounds. Why?

The identity management, content management and digital rights infrastructure touches many different applications and infrastructure within the utility. It therefore is much more than buying some software and placing it on a highly available server infrastructure. It often requires re-engineering of applications which takes time, money, resources and excellent testing before moving into production. Management should take note of this.

The utilities should band together and create an XML schema for smart grid data. This will allow for easier, lower cost data management between the utility and third parties as well as provide for better and more seamless content management enforcement of the data.

About the Author

Guy Huntington is a learned and burned identity management and security consultant. He has led a utility identity management program, participated in a utility security assessment, integrated physical and logical security and rescued several large Fortune 500 identity projects. His white papers can be read at <http://www.authenticationworld.com/papers.html>. He can be reached at guy@hvl.net or 1-604-861-6804.