The Institution of **Engineering and Technology**
Michael Faraday House
Six Hills Way, Stevenage
Hertfordshire, SG1 2AY
United Kingdom
T +44 (0) 1438 313311
F +44 (0) 1438 765526
www.theiet.org

Ref: (S)917:HF

Smart Metering Implementation Programme – Roll-Out Team
Department of Energy & Climate Change,
4th Floor, Area D
3 Whitehall Place,
London,
SW1A 2AW

17 October 2011

[redacted]

Smart Metering Implementation Programme:
Call for evidence on Data Access and Privacy

Please find attached the response from the Institution of Engineering and Technology to the call for evidence.

As befits a highly inter-disciplinary topic such as this, the response has been prepared by the IET's Energy Policy Panel in collaboration with the IET's Policy Panels on IT, Communications and Transport.

If we can be of further assistance to the Programme please do not hesitate to contact us.

[redacted]

Smart Metering Implementation Programme:

A call for evidence on data access and privacy

Response from the Institution of Engineering and Technology (IET)

INTRODUCTION

Smart Metering is mandated to comply with EU Directives but the real prize in terms of meeting the UK's Climate Change, Security and Affordability policy goals is *Smart Grid*. Interpretations of the words "smart grid" can vary but looked at from the customer end of the telescope it is much clearer: it means making it transparent and easy for customers to flex their electricity demand in response to the availability (and thus carbon intensity) of electricity, thus improving security of supply for all, keeping down costs for all, and reducing climate change impacts – and that they should be rewarded for their contribution.

Demand data is going to be critical to the future operation of both the grid and the market. It follows from this that (a) the smart metering programme should be designed with an architecture that provides end to end security consistent with future smart grid applications and (b) the programme must be successful in terms of public engagement and acceptance.

Both Suppliers and DNOs will need to put in place robust measures to ensure that privacy and security is 'designed-in' to data handling systems and processes. The same follows for any 3rd parties (intermediaries) such as Commercial Aggregators or Virtual Power Plant (VPP) operators that in future might aggregate (and/or control) consumer half-hourly (hh) profiles for trading and/or balancing services.

Looking to the medium term future, if the data is ever going to be useful in the management of instantaneous loading, such as controlling EV charging, then near real-time data will be needed.

There is currently a high degree of uncertainty around smart metering and the Foundation Stage must be used for debate and research into how consumers might engage with smart meters (for good or ill), how the meters will interface with other equipment in the home and how the system can link into other systems needed as part of a *Smart Grid*. Without customer engagement and effective interfaces with other equipment, the Smart Meter programme will be little more than an expensive remote meter reading application.

Currently there appears to be no explicit or implicit adverse customer reaction to providing access to more granular data. This position will be heavily influenced over time by how industry uses the data, for example whether customers see the value or not and whether there are issues over unwanted marketing. If the initial introduction of the Smart Meter initiative misfires, the industry is not likely to be given a second chance.

THE PRIVACY POLICY FRAMEWORK

Consumer Views

1. Please submit any further evidence, such as surveys or consumer research, regarding privacy issues and smart metering. In particular is there evidence available about the effects of the availability and aggregation levels of more granular data (for example daily)?

Alliander in the Netherlands has become the first distribution grid operator in Europe to receive a Data Privacy and Security certification and is one of the best examples of research and trials to have completed and documented real evidence.[1]

Alliander (formerly Nuon) unbundled in 2009 and formed separate Production/Supply and Network companies. Metering is part of the network company (DNO) responsibilities. The granularity of the data collected is not in the public domain but it is clear from discussions that there is a similar level of detail involved to that under discussion in the UK. The data is used both to inform the customer **and** to provide the utility with operational data to manage their network. Of particular interest in the context of this consultation is their customer engagement programme before the trails and the number of their customers willing to go on film to confirm the success of the trial.

Being a first mover in this Privacy Certification task, Alliander faced several challenges. However, by systematically overcoming these hurdles, Alliander has learned valuable lessons that it is now able to share with other players in the electricity market. For further information see Annex A.

Competition Impact

2. To what extent would different rules for access to data between suppliers and third parties be expected to impact on the development of an energy services market (in terms of product and tariff innovation and / or entry to the energy market by third parties)?

If the data privacy and security measures are contrived in such a way that the barrier to entry is prohibitive for all but the 'traditional' stakeholders, then by definition these market opportunities would be lost and competition reduced.

The opportunity for a market to evolve in this space is dependent on the ease by which third parties can obtain data, utilise it and influence the equipment on the home area network (HAN) side of the Smart Meter via the Smart Meter. The time delays in an operator receiving usage data (possibly aggregated at the area or regional level) and sending messages that influence consumers' appliances (such as EV battery chargers, freezers or electric heating systems) will be critical. Excessive delays in this process risks destabilising the power system with potentially catastrophic results.

What are the particular data uses to which these concerns apply?

Other stakeholders may evolve that are neither retailers nor network operators and may be able to provide community level services that are used solely to provide balancing or ancillary services on a local basis rather than on a DSO level. Energy Supply Companies (ESCOs) and Virtual Power Plants (VPPs) are likely to provide necessary innovation in low carbon energy supply business.

Micro-grids that are in fact supported by the distribution grid rather than the main provider are a possibity (e.g. similar to Woking housing estates[2] that have no utility tails from a DNO but are provided by private wire solutions).

---

[1] "Data Privacy and Security for Smart Metering - Alliander Certification Case Study", EIOS52T, 2011).

[2] Borough of Woking: Local sustainable energy systems: http://www.woking.gov.uk/environment/climate/Greeninitiatives/sustainablewoking/lses

3. Are there any data uses, apart from those set out below, where the arrangements for access to data could have an impact on the benefits of the programme?

The assumption in the consultation is that the only way Smart Metering is going to deliver energy efficiency benefits is by consumer behaviour change. Experience indicates that tipping points in consumer behaviour do not follow rational decision making. The reliance on human behaviour to deliver the majority of benefits expected from Smart Metering is thus at best tenuous, at worst very expensive.

The Programme misses an opportunity by not allowing for automated use of real time Smart Metering data. For electricity, there are other significant opportunities, mostly to do with automatic active network management providing real time improvements to the operation of the distribution and transmission grids.

In addition, it would be a missed opportunity if the programme does not include the opportunity for dual fuel users to automatically switch between the different fuel vectors as a means of utilising water and space heating as flexible demand options. More integrated data analysis would require greater clarity than half-hourly usage if real time balancing is going to take place at a residential/small industrial level (and in great enough numbers to have a useful impact.)

How does this analysis differ for the gas market?

The IET does not have the expertise to comment in detail on the gas market. However, we wish to draw attention to the future significance of optimising use of electricity and gas within the home or small industrial setting. ESCOs or others could be expected to develop arbitraging services for consumers between electricity and gas energy (and domestic heat storage e.g. as hot water storage) depending on tariff signals.

Energy Efficiency

4. What types of energy services and energy advice could be provided by the market (by suppliers and / or ESCOs / potential new entrants) that require access to specific levels of data? What level of data granularity (frequency, time-lag) are needed to provide such services and what is the potential impact of these services in terms of percentage energy savings? Please provide empirical examples and explain the basis of any assumptions and distinguish between gas and electricity.

While some studies indicate that customers trust their energy supply company to provide energy efficiency advice, others such as the recent study by Ernst and Young[3] indicate that customers do not understand why suppliers want them to consume less and might prefer to receive this information from sources they perceive as more neutral.

For electricity there is a potential wide market for energy efficiency advice. This can currently take two forms which should not be confused:

- Suppliers can drive customer engagement in energy usage through analysis of actual energy consumption (read data) and home/behavioural data (third party and customer supplied data). Such analysis can be fed back to customers through a variety of media, such as an energy saving report, supported by energy saving tips, alerts and products to aid energy reduction. The Smart Metering programme provides accurate meter readings with a mandated requirement that you provide your data to the supplier.

[3] "The Rise of Smart Customers: how consumer power will change the global power and utilities business: What Consumers Think", Ernst and Young, 2011 http://www.ey.com/GL/en/Industries/Power---Utilities/Seeing-energy-differently---Smart-customer---Consumer-research

- The availability of so called clip on monitoring devices which give closely approximate readings and, if you choose to pay for it, the convenience of downloading data on the move or to personal computers. You choose to share your data either when you buy your clip-on, or through subsequent opting-in (depending on the make and model of clip-on). People feel that they "own" the data and have made a choice of their free will to trade it in return for certain benefits. However they are not in an informed position to know any potential privacy dangers of services running off commercial clip-ons.

The bottom line is that the privacy and data security of both options need to be assessed.

For gas, the options are currently limited to those provided by the Supply Company because there is no readily available technical means of detecting the amount of gas flow at domestic level other than though the gas meter.

Theft

5. Should theft management be considered a regulated duty for which suppliers should have access to a certain level of smart metering data? What level of data would be required and how would this be used to manage theft? Please provide practical examples.

It seems logical for this to be a regulated duty as energy thieves are unlikely to opt in.

The Theft Act 1968 is the overarching legislation for these offences. Suppliers will have a requirement to assess the 'leakage' of electricity and where this becomes an apparent offence will pay closer attention to any losses. The 'tipping-point' re any loss will be dependent on individual suppliers however a substantial loss is a commercial issue and one that will not pass undetected for too long. A specific offence of 'Abstracting Electricity' has been included in the Theft Act and was drafted with the intention of ensuring that the dishonest deviation of electrical supply was illegal i.e. 'by-passing' the meter. In most instances this was intended to prevent home-occupiers using physical means e.g. 'loop-wiring' to secure electrical supply without it being recorded. However with the introduction of smart-metering this will entail alternative means to identify where/when/how and the amount of an electrical supply diversion had occurred. Conventional abstraction is easy to detect – either physical evidence of tampering and/or comparing the amount of electricity against the meter reading. 'Smart- metering' would require a similar comparison process to be devised whereby the prosecuting authorities would be satisfied.

Daily readings are sufficient for theft prevention and detection. This would provide Energy Suppliers with a regular set of meter readings from which they can proactively detect unusual consumption patterns but does not require more granular consumption information.

Where theft can be shown to have occurred, using the test above, detailed meter data should be examined by the police, with the usual safeguards. It would seem illogical to install Smart Metering with half-hourly data gathering per household and then not be able to interrogate the data at this level of detail to identify fraud. However, large apartments and flats may prove more difficult to regulate in this way and may need to be regulated to allow sufficient granularity within a building[4].

Enel (Italy) paid for their Smart Metering implementation in record time due to the benefit afforded to the DNO by debt recovery as a result of the Smart Metering roll out. This was achieved because of the granular level of detail available.

[4] For example, communications to smart meters in basements of flats may be problematic requiring special arrangements and it's more difficult to prove who has tampered with a supply located in the common areas of a shared building.

6. Does data need to be collected from all customers all of the time, for theft management, or could there be a trigger for accessing more detailed data (for example where theft is suspected)?

For Energy Suppliers to deliver the maximum benefits attributed to theft detection and prevention, they must have the ability to collect data from all customers, all of the time. The technical specification for smart meters includes a number of alarms to highlight meter tampering but these will only be triggered if there is possible tampering of the smart metering equipment itself. Experience has shown that energy theft often occurs away from the meter, such as on incoming electricity cables. In these situations a meter tamper alert would not be triggered and no one would be aware that energy theft is taking place.

Data retention is an issue here, however as this is an on-going commercial requirement, access to the data would have to be agreed between the supplier and the investigating body – e.g. the police service.

Time of Use Tariffs

7. What level of take-up of time-of-use tariffs could be expected under different scenarios for access to data?

The development of ToU tariffs will be an almost inevitable consequence of the need for both DNOs and Suppliers to be able to influence load shape to either control peak demand or induce flexible demand to follow wind generation forecasts and other supply side variability.

However, the question assumes people standing by their In Home Display (IHD) to follow the wind generation pattern 24 x 7 and then acting rationally on the information. We would re-iterate that to deliver widespread time of use benefits will require some automatic real-time connectivity and feedback.

Public information needs to be provided to educate customers about why time of use tariffs are of social value before useful data on likely take up can be obtained.

What information is needed to design time of use tariffs? In particular would sample or anonymised data be sufficient?

This is a more complex problem than it appears at first sight. The complicating factors are:

- this needs to reflect both supply side and network constraints which will be challenging in the current industry structure where supply/demand of energy is separated from network. What would happen if EV charging at a time of supply surplus was constrained off by network constraints, and could not be delivered later on because of supply side constraints. Whose fault would it be? Who would the customer complain to and what would be their redress?

- In the long-term future when/if plans for EVs, heat-pumps, micro-CHP, solar PV, domestic wind turbines, etc. take off at scale, it seems likely that the DNOs might need to manage the loading and connected generation on a section of their network. If this is to be achieved through the price mechanism, then the tariff will have to be set locally, rather than being determined by a national electricity retailer. (Particularly so if sale of electricity from EV batteries back into the grid (V2G) is proposed.) This points to the need for geographical granularity in whatever solution is adopted.

In the short term it may be sufficient for Energy Suppliers to require access to an aggregated level of half hourly data from smart meters in order to deliver the innovation in the provision of new products, services and tariffs including Time of Use (TOU) for their customers.

A lot more study is required to devise a system of time of use tariffs to deal with the low carbon energy system envisaged from 2020 onwards. By then it can no longer be assumed that time-of-use tariffs will be nationally managed by electricity retailers who "share" the distribution network. If we are to avoid expensive rebuilding of the electricity grid when/if heat pumps become the system of choice for many homes, the tariffs will have to be locally set to even out the **distribution** load, not just the national **generation** load. There will also be a need to ensure ToU tariffs do not cause "herd" behaviour where, for example, sending a message of a reduced tariff would trigger large-scale automated switch-on of EV battery chargers.

Settlement

8. Do you agree that individual half-hourly data is not currently required for suppliers to meet their obligations in relation to settlement? Over what timescale are any changes to settlement likely to take place and what might the implications be in terms of data requirements?

Although time of use (ToU) tariffs don't yet need to be designed to individual half-hourly time bands, it makes sense to settle on actual half-hourly data rather than continue to use assumed profile data taken from volumes in each ToU time band (e.g. demand taken over several hours). That in turn would require Suppliers to retain half-hourly data - but it would still be aggregated for settlement.

Retaining half-hourly data at the consumer level obviously becomes necessary if we eventually move to **billing** on a half-hourly basis. This may seem far-fetched at the domestic level but given the likely future spot price movements and ramp rates once we approach target wind generation capacity, there is every incentive for Suppliers to move towards that objective as soon as it becomes practical to do so. This would logically lead to the development of dynamic tariffs which would potentially set forward prices on a half-hourly basis to reflect 90 minute ahead forecast (i.e. pre-gate closure) volumes and hence spot prices.

Wholesale Hedgeing

9. How far would aggregated or sample data provide suppliers' with what they need in the area of wholesale hedging? Please provide examples of how the data would be used and where possible quantify potential benefits and costs.

Not answered.

Debt Management

10. What level of data would be required and how would this be used to manage debt? Please provide practical examples.

Not answered.

11. How would suppliers envisage using daily data to support debt management and what evidence do they have to support claims of additional savings that could be achieved with access to daily data as opposed to less frequent data?

Not answered.

Vulnerable Customers

12. How could smart metering data be used to identify and protect vulnerable consumers? Should such activity be considered a regulated duty and are any licence changes needed to create particular duties on suppliers in this area?

Detailed consumption data in itself would not necessarily help Energy Suppliers in identifying vulnerable customers as this is purely metering data. In order to identify a vulnerable customer, Energy Suppliers would need to be aware of the customer age, whether they had young children and their ages and details of disabilities etc – none of which will be available from the smart meter. This would clearly represent an unacceptable intrusion into individual privacy, unless the customer elected proactively to provide such information to allow a supplier to provide some level of e-monitoring on this basis (for example for an elderly person living alone).

Network Companies

13. Do you consider that use of data by network companies to support them in maintaining an efficient and economic network should be considered a regulated duty?

Yes. DNOs already have a regulatory duty to 'develop and maintain an efficient, co-ordinated, and economical system of electricity' (Electricity Act). It follows that they should have access to the smart metering data needed to support the development of the low carbon infrastructure. It is important for customers and all players to understand that the addition of the demand side is not for the sole benefit of the DNO: the benefit is that consumers will get paid for their services and that all users will benefit due to reduced running costs.

This does raise the question of timely data collection. If data is purely going to be used to plan the distribution networks for the future (as has been traditionally done to build fit-and-forget networks), there is likely to be little or no immediate benefit to customers. If on the other hand the data can be used in real time to make a real difference to a customer's situation straight away, it has a much greater chance of selling this benefit to the customer as a "must have".

This is an exceptionally important area for DNOs in terms of the extent to which they will have access to data for network management purposes. Granular and 'location specific' data will be essential for network companies or their specialist providers /aggregators to address real time network active management. This is not only domestic or commercial demand but also distributed generation output and the management of distributed storage. It might also extend to an interaction with the householder that enables the power electronics in their AC/DC interfaces to provide network conditioning for power factor, voltage or waveform.

A key issue here is to understand that at present the capacity of the distribution network relies on a variety of small loads at different times averaging out the capacity required. However new developments such as EV charging have the potential to result in large 'mobile' loads to appear at no notice. This will make balancing of the network much more challenging and require a range of locally based control and feedback mechanisms.

As networks move away from today's 'fit and forget' type of operation to requiring active control, this can only be undertaken with adequate data that enables network observability.

14. Do you agree with the requirement for such data to be anonymised or aggregated wherever possible, and how should this be monitored?

Given the sensitivity worldwide to Smart Metering abuses, it will be essential for people to have confidence that data is being used and controlled in as safe an environment as possible. However, this should not preclude the data actually being used to achieve optimum return for the customer both economically and from a societal standpoint.

To achieve this will involve education, communication and delivery of credible, high integrity project roll-outs. Given the 'sell' that is being done to the public on the benefits of smart meters, they will not understand if the reason those benefits are not realised is because the industry was unable to use the data it collected in an optimum manner.

Recognising the sensitivity, the Energy Networks Association (ENA) has commissioned a Privacy Impact Assessment (PIA) which is now at an advanced draft report stage. An important provision of the PIA is that for network management purposes the half-hourly demand profile data would be aggregated in order to 'build' a demand profile for a specified section of a network - typically an LV feeder or possibly a branch. As such, the data would be depersonalised (not address specific) which should remove any reasonable concerns over privacy.

If customer data is used for these purposes, then the network operators should be strictly liable for notifying and compensating customers in the event of any privacy breach, whether through leakage of personal data or through re-identification of pseudo-anonymised or aggregated data.

It might it be possible to differentiate between 'general consumers' and those who consent to more granular or personally identifiable data? In the case of energy, the more granular data would by definition have some added value for the retailers or networks or third parties, so this could in principle enable something to be 'offered back' to the consumer that provides it.

Allowing customers easy access to their data in the home requires the right balance between ease of use, otherwise customers will not be engaged, and applying the appropriate security and privacy levels. The approach should ensure only a minimal amount of effort is needed from customers to allow an Authorised Third Party (ATP) to access their data using the DCC.

All Authorised Third Parties should be signatories to the Smart Energy Code and obtain a Data Privacy and Security certification similar to the Alliander example in order to obtain access permission from customers.

15. Would suppliers be expected to advise consumers of network company usage of data given network companies do not have a direct relationship with customers?

Every use of customer data (i.e. by which companies, for which purposes) should be notified to customers by whoever controls access to the data – presumably DCC.

It is essential that customers know who is using what data and are able to have the opportunity to opt-out if desired. An incentive should be provided to ensure as many people as possible remain opted-in.

Choice Mechanisms

16. Are there any alternatives to a basic opt-in or opt-out approach to consumer choice such as some form of prompted choice? What are the practical and consumer protection considerations in relation to different options (for example when and how)? From a

consumer perspective what alternative approaches and vehicles (for example letter, email, phone) to seek customer consent are there?

The Alliander experience (see Q1) is a good model for identifying many different options for seeking customer consent.

17. What evidence is there of likely take-up rates that could be achieved through different approaches to consumer choice?

The Alliander (see Q1) experience is a useful reference given the length of time this process has been running and the success of their achievements.

Data Minimisation

18. What current and future technical options exist for energy consumption data minimisation / privacy enhancing technologies? How might aggregated or anonymised data be provided in practice? Would this imply additional services to be provided by DCC?

By definition, if the DCC is collecting all data it is an exceptionally critical hub with huge data security and privacy issues. If data is to be served to distributed data groups (e.g. to a DNO) then the reduced data set has less significance and hence less sensitivity. It is highly likely that future technologies will allow security/privacy policies to be implemented in a distributed and yet coherent manner. There is no need for all data to be sent or stored centrally. Data transmission minimisation will also have benefits in data capacity requirements and latency to distributed nodes on the network. A distributed DCC architecture would make this a lot less problematic.

CPP Group plc (CPP) is already proposing some sort of central trusted clearing house for useful anonymised re-purposed statistical data from many sources. It would be worth looking into this example to see if it suggests a way forward.

The Regulatory Approach

19. What parts of the privacy policy framework do you think should be delivered by regulation and why?

The privacy policy is part of the security policy for the smart grid and should be regulated The security marking for the data should be proportional to the possible aggregated damage that leakage of the data could lead to. This would need further consideration, but a starting point for discussion could be that monthly household aggregated data deserves PROTECT marking with daily data being RESTRICTED, half-hourly individual data being CONFIDENTIAL and perhaps datasets for many households being SECRET.

In addition, caution is required regarding who is allowed what level of data and what is transmitted and held centrally.

20. What is the most effective way to set out any sector specific protections around privacy (e.g. licence conditions or other alternatives)?

There is clearly a political, legal and public confidence imperative that data privacy should be protected. But there is another side to this coin. Data gathered on this scale is unique and potentially valuable, not just commercially but socially and for future public policy. Some of that value is only realised by combining the smart meter data with other data about households. It is

a privacy mine-field and it is doubtful that the collective wisdom on tap today is enough to get this right **in one pass**. So we need some flexibility built into the legislation.

DATA ACCESS

Access to data via the Smart Metering equipment in the home

21. What practical options for authentication would provide the right balance between allowing easy access to consumer data in the home while providing the necessary privacy protection? Are there any other issues or options that the programme should be considering in developing the approach in this area?

The Programme misses an opportunity by including little or no expectation for real time use of Smart Metering data. For electricity, there are other significant opportunities, mostly to do with automatic active network management providing real time improvements to the operation of the distribution and transmission grids.

The development of Time of Use (ToU) tariffs will be an almost inevitable consequence of the need for both DNOs and Suppliers to be able to influence load shape to either control peak demand or induce flexible demand to follow wind generation forecasts and other supply side variability.

The question assumes people standing by their In-home Display (IHD) to follow the wind generation pattern 24 x 7 and then acting rationally on the information. However, we would re-iterate that to deliver widespread time of use benefits will require some automatic real-time connectivity and feedback.

22. Are there other issues that need to be considered to make using the HAN a viable route for access to data in the home, from either a process or consumer perspective?

This really is a major element in ensuring the Smart Meter is a gateway for the Smart Grid to deliver its benefits so the answers to question 21 above and also questions 3 and 7 are highly relevant here.

Another possibility in the future, may be that the HAN may well **not** be providing data to the DCC but controlling home appliances, including heating and EV battery charging in line with algorithms determined by the householder, based on real-time tariff information received from their electricity retailer. Integrity of such data received from the external network, interpreted by the Smart Meter and fed into the HAN will therefore be crucial. Corruption of tariff information, whether accidentally or maliciously, could be seriously detrimental to the householder and could seriously disrupt the grid, particularly if it is used to request reverse power flows, such as in Vehicle-to-Grid applications and control of high levels of renewable energy.

Access to Data via DCC

23. What sort of arrangements would provide an appropriate balance between providing ease of access for consumers seeking to sign up to new services and adequate protection for consumers' data when accessed via DCC?
Do you have any suggestions for alternative approaches?

By definition, if the Data Communications Company (DCC) is collecting all data it is an exceptionally critical hub with huge data security and privacy issues. If data is to be served to distributed data groups (e.g. to a DNO) then the reduced data set has less significance and hence less sensitivity. It is highly likely that future technologies will allow security/privacy

policies to be implemented in a distributed and yet coherent manner. There is no need for all data to be sent or stored centrally. Data transmission minimisation will also have benefits in data capacity requirements and latency (the time it takes for “real time” messages to reach distributed nodes on the network).

As indicated elsewhere in this document, the DCC approach has many short-comings and even greater concerns regarding data privacy and integrity. A better alternative would be to send specific data directly to the points in the supply chain that can operate on that data. No one group then has the complete picture.

Foundation and Non-Domestic Customers

24. Are there other issues or options that the programme should be thinking about for the Foundation Stage or for non-domestic customers to facilitate access to data?

Not answered.

25. Do you have any suggestions as to how the Foundation Stage can be used to further learn about our approach to data access and privacy?

Not answered.

ENDS – but see Appendix overleaf

Alliander - A Case Study

Alliander in the Netherlands has become the first distribution grid operator in Europe to receive a Data Privacy and Security certification and is one of the best examples of research and trials to have completed and documented real evidence.[5]

When, on April 7th 2009, the Dutch Minister of Economic Affairs repealed the proposed mandate for smart metering deployment due to data privacy and data protection concerns, Distribution System Operators in the Netherlands were forced to re-evaluate the smart metering projects (mainly pilot projects) they had been working on. Since the interruption, Alliander has continued to pilot smart metering, offering smart meter replacements as a service to its customers, either for new delivery points in new/refurbished constructions, or simply at the request of its clients. However, Alliander very quickly realized that it had to look for new approaches to address consumers' concerns about data privacy, hence it undertook a project to become "certified compliant" in its deployment of smart meters. Two years and €2 million later, in February 2011, Alliander (more precisely its business unit Liander) has become the first distribution grid operator in Europe to receive a Data Privacy and Security certification.

The project[6] began in August 2009 and was closed in January 2011. Alliander collaborated throughout with auditing firm PricewaterhouseCoopers (PwC) and IT Service provider Accenture.

Alliander identified over 300 detailed criteria that needed to be complied with, and introduced four areas of measures and "controls": technological, procedural, organisational, and policy controls.

- The Technological Controls affected every aspect of Alliander's smart metering solution from the M-bus devices, to the smart electricity meters, to the data concentrators, to the communication network, to the final central system, and included wireless encryption, radius, pairing of devices, tamper detection, DC activity logging, firewalls, etc…
- Procedural measures were implemented in four macro areas: Technology, Contract management, Meter rollout, and Meter operations. The procedural measures include: Data collection permission registration, Encryption key update, Incident / problem management process, Event management, Information Security and Privacy Management System + reporting, Right to access (and correction) consumer data.
- Alliander's organizational controls affect three areas: Data privacy owner, Privacy Officer and Information Security Manager and responsibilities of employees.
- Finally, Privacy and security guidelines were created and documented in policy documents approved by management.

The first round of the auditing phase, which was carried out in August 2010 revealed a couple non-conformities that needed to be addressed and fixed before obtaining certification.

[5] Entry posted March 30, 2011 on http://idc-insights-community.com
by Roberta Bigliani , tagged EMEA, Security, Smart Grid/Smart Metering, Utility Industry
Title: Alliander: first DSO to receive Data Privacy certification for Smart Metering

[6] (for a detailed project description refer to IDC Energy Insights document "*Data Privacy and Security for Smart Metering - Alliander Certification Case Study*", EIOS52T, 2011).

- The first non-conformity referred to a Privacy issue. For smart metering pilot installation, Alliander made the assumption that technical data was not personal data, however, while there is no specific final jurisprudence on this matter, for auditing purposes PwC considered technical data as personal data, and for personal data handling the law prescribes that clients need to be informed. As a result, Alliander started a cast client informing process, involving 46,000 letters sent out in a 2-week period with 327 calls in response. It is interesting to mention that only 2 clients refused the smart meters.
- The second non-conformity referred to Data Security issues. Intrusion tests revealed security issues in a specific group of installed smart meters and no adequate actions were available to mitigate the risk. Replacement could not occur in time for the audit, so Alliander physically removed all communication between the meters and the data concentrators, basically operating the smart meter as a 'traditional' meter. Alliander will replace this population in 2011.

The final Evaluation & Closure stage of Alliander's data privacy and security certification project started in December 2010, and ended in January 2011. This included evaluating Alliander's privacy readiness, through additional questioning by PwC, the creation of a final report, and concluded with Alliander handing over the Management's Letter of Intent. **On February 14, 2011 Alliander's DSO Liander obtained Privacy certification, becoming the first distribution grid operator in Europe to receive it.**

Although the project is finished and the Privacy certification is achieved, the Security and Privacy processes require ongoing attention and management. In order to manage the processes in place, Alliander established an Information Security & Privacy Management System (ISPMS). ISPMS carries out several ongoing tasks, including: single deviation register for all actions, due dates, owners and mitigations, bi-weekly meetings for progress monitoring, consolidated reporting to responsible management, and follow-up by a dedicated Privacy Officer and / or Information Security Manager.

Being a first mover in this Privacy certification task, Alliander faced several challenges. However, by systematically overcoming these hurdles, Alliander has learned valuable lessons that it is now able to share with other players in the electricity market.