



Smart Metering Prospectus

Data Privacy and Security

RWE npower

Trigonos
Windmill Hill Business Park
Whitehill Way
Swindon
Wiltshire SN5 6PB

T +44(0)1793/87 77 77
F +44(0)1793/89 25 25
I www.rwenpower.com

Registered office:
RWE Npower plc
Windmill Hill Business Park
Whitehill Way
Swindon
Wiltshire SN5 6PB

Registered in England
and Wales no. 3892782



Question 1: Do you have any comments on our overall approach to data privacy?

- We understand the distinction between privacy and security, and believe that security of supply should have the highest precedence
- We believe that the Data Protection Act, the Privacy and Electronic Communications Regulations and the European Convention of Human Rights Article are sufficient, and that any further regulations and codes should contextualise them rather than add to them.
- We feel that there is a risk that “regulated duties” may be drawn too narrowly and may therefore reduce the social benefit of smart metering
- We believe that smart meter mandation before DCC Go Live presents real privacy and security risks

Privacy by design – We support the principle within RWE npower, we are conducting an exercise to ensure that privacy and security are designed in to our own systems.

Prescription - Whilst we support the principle behind Ofgem’s proposals we have concerns in relation to how prescriptive Ofgem is intending to be in relation to access to and the use of customer data. If too many restrictions are placed on the suppliers’ ability to use the data that smart meters will generate then it will inhibit their ability to develop new products that are more reflective of how energy is consumed by a customer. Whilst allowing customers the absolute right to determine how their data is used is in principle correct how this is implemented will have profound effects on the ability of suppliers to develop new products and has the potential to stifle the benefits of the additional data smart metering will provide.

Data Protection Act - All smart metering is doing is providing an additional subset of data (being additional consumption data at an half-hourly level). Suppliers currently handle and process vast quantities of personal data and seek to do so in compliance with the Data Protection Act. We agree that customers’ privacy should at all times be protected. However, we believe that the Data Protection Act is the best way forward to ensure the correct use of the additional data smart meters will provide. We already have obligations under the Act to ensure our use of such personal data is legitimate, is not excessive or held for longer than is necessary and customers are made aware (through the contractual arrangements we have in place and the privacy notices on our websites) why we are processing their data and to whom that information may be shared.

Consent - We would suggest that a consent only based approach is flawed and will prevent the very innovation that the introduction of smart metering was viewed as being able to provide that aside managing such consents would be complex and costly and potentially require fundamental changes to suppliers’ systems.

The distinction between privacy and security. We do not seek to add new nomenclature but for the purposes of this document, define privacy and security as follows;

Privacy: The need to ensure the confidentiality of customers’ personal data to the extent that they are able to conduct their lives without undue intrusion, in line with UK and European law.

Security: Tools and techniques that ensure the confidentiality, integrity and availability of an entity that has some value to its owner



National Infrastructure – We believe that the smart metering system should fall within the purview of the Centre for the Protection of National Infrastructure (CPNI). Exposures of risks are;– i) systematic curtailment of electricity supply leading to an effective blackout, ii) systematic cycling of curtailment in such a manner that it presents a challenge to the ability of power generation to respond to the load change and/or presents a challenge to the resilience of the synchronised alternating current in the grid, iii) use of some part of the metering system as the back door into some part of the distribution grid, transmission grid, or other item of critical infrastructure.

Smart Grid – We support the development of Smart Grids, and have stated consistently that the smart grid development should run alongside the smart metering programme and be recognised by it. We recognise that not only could activity at the meter threaten security of supply, but that the household metering system could be used as the back door into the grid. Whilst smart grid development will generally improve the resilience of national infrastructure, there is specific exposure to hacking if communication of the meter, DCC or suppliers to the networks is two way. We believe that it is for the Energy Networks Association in particular to determine the exposures.

The control of access- Public access is different at different points in the chain. For example a GPRS signal can be physically received by any device, but useful receipt or malign interference can only be effected if the perpetrator has access to the protocols generally and the security (e.g. passwords and decryption) specifically. We note that the challenges of data latency and of information storage and process will to some extent mandate a choice between the relative importance of privacy and security. For example a data rich carriage of personal data with a highly configured specification for access (e.g. organisations A and B can access data elements X and Y), in its requirement to be delivered within a system of certain size, require a reduced level of encryption (e.g. encrypt less information, use less secure encryption,) to manage latency or centrally stored data.

Best practice – We feel that the stated current proposals and indicated future work are entirely appropriate at this stage in the programme. Referencing a range of UK Government and international good practice, as well as lessons learnt from other implementations, provides a sound basis for security to be addressed correctly as the programme progresses and matures.

Central security body - The benefits of having a centrally managed independent body managing the security testing and accreditation for all aspects of the system should be seriously considered. Standard testing and accreditation arrangements, should lead to optimised cost and ensure that common agreed standards are adhered to.

HAN – We have particular concerns about the HAN. The HAN signal can be accessed by unauthorised parties within the home and near the home. We suspect that much can be learned from recent experience with wi-fi. The HAN will need strong security standards, particularly if the IHD (or other device) were to communicate two way with the meter. If the consumer is allowed to connect physically or virtually to the HAN, this connection should be read only access.

There is also a concern around verifying that devices that want to join the HAN confirm to specific security standards and do not weaken the security of the HAN and the other devices in it, especially the meter and the data it contains. These smart devices may be manufactured in many different countries, often as cheaply as possible. Supply chain security is an issue here.



The disposition of redundant data – It is hard at this stage to know which long term data will be most useful. For example, the National Grid demand forecasts use aggregate data going back more than 17 years, for the purpose of trend analysis. This would be much informed by a more granular view (for example gross and net import, urban vs. rural differences, time of day differences, and even with cross reference against building type, fabric change such as insulation, and occupancy). The considerations for long term storage are data protection regulation, storage costs, and processing costs. Broadly speaking, it is our view that privacy is less of an issue for older data, and that cost should be a key consideration in data storage or deletion.

Access control – we agree that the DCC should determine control of access to data carried by the DCC. Where a consumer wishes to allow configured access of parties to data pertaining to their consumption, that this should be managed technically by the DCC. We do not believe that consumers should have direct access from which to configure access control.

Event management – The DCC has a role in security, for example network monitoring and incident response management. Broadly speaking, we believe that security should be prioritised, and any compromise on security from privacy considerations should be considered very carefully.

The voice of consumers – We note that some of the media, some consumer advocates, and some single campaigners, have been vociferous on the matter of privacy. Whilst all views should be given due consideration, we note that there is little evidence that consumers are as concerned about certain aspects of privacy as they are represented to be. We believe it to be essential to test the views of actual consumers, and this should be executed and then analysed impartially.

Meter specification - The Functional Requirements Catalogue and the Technical Specifications and their incorporation into the Smart Energy Code are essential.

Proactive management of privacy - The benefits of extending the DCC responsibility to include the proactive management of privacy and security should be considered.

Risks in the interim period – we believe that the most secure operational model would have the DCC going live from day one. The extra risks, mitigations and cost around the DCC not being in operation until 2013 and any interim solution need to be clearly stated,

Additional areas of concern are i) who will check compliance with common technical specification, ii) who will manage incident response prior to the DCC being up and running?, iii) there is a cost to migrate to the DCC while minimising risk during change and subsequent further change to rationalise / standardise and then check and ensure security of the final arrangements is as expected.

Longevity of the design - The specification now for privacy and security must be fit for purpose for the next twenty years. Policy development should not be precluded. For example, it is very likely that the DCC would be a good place to hold primary keys that link to databases for Feed in Tariff installations, Green Deal installations, and installations conducted under the Carbon Emissions Reduction Target and the Community Energy Savings Programme. These are not in the current DCC scope.



Question 2: We seek views from stakeholders on what level of data aggregation and frequency of access to smart metering data is necessary in order for industry to fulfil regulated duties.

- We believe that the specification of regulatory duties is unhelpful as it implies very narrow responsibilities, and if used, must be broadly drawn
- Managing a customer's account to their best interests and with respect to the sound management by the supplier, will require more information in the future and indeed this is the great benefit of smart metering.

Clarity – we note that the terms “regulated duties”, “regulatory duties”, and “regulatory purposes” have slightly different meanings. We believe that “regulated duties” (and similar terms), should be broadly drawn to include activities that may have social purpose or which may benefit the consumer, or which may at some later point be useful for society or consumers.

Duties of consumers - We note that consumers have regulated duties, for example under the Electricity Act 1989, Gas Act 1986, and the Distribution Code. At some risk of simplifying, these duties are not to consume energy without a contract to pay for it, and not to install items with substantial electrical consumption and which overload the network. In practice, these responsibilities commonly discharged by suppliers, for example by deeming contracts. We expect this to continue, and this will require supplier access to relevant consumer data.

Access by suppliers to half-hourly electricity data – The electricity market balances at half-hourly resolution. It is essential for energy policy that the electricity system develops over time towards half-hourly resolution for all meters. The cost of a bulk change to half-hourly settlement at this point would exceed the benefits, and suppliers will develop pockets of half-hourly management, where the consumer value is greatest. They therefore need access to half-hourly data for some meters but no regulatory duty at this time to process it for others.

Access by suppliers to sub-half-hourly electricity data – Whilst it would be quite possible to settle the system at higher resolution (for example five minutes), we believe that half-hourly is the right resolution for energy meter data en masse for the next thirty years at least. There are likely to be instances where higher resolution is required (for example to meter demand side response at higher resolution). At this point in time, designing this into the smart metering system is too complex, and such metering would have to be outside of smart metering. An example is the provision of frequency response by domestic consumers and the wholesaling of this to National Grid. The verification of this provision could be through audit of the device providing the response, and/or by sampling. In general, there should be no regulations at this stage that preclude or limit the abilities of suppliers to innovate.

Access by suppliers to other electricity data – There are a number of other data types, such as reactive power and harmonics. In general, there should be no regulations at this stage that preclude or limit the abilities of suppliers to innovate. We believe that the data protection act provides all proper guidance.

Access by suppliers to daily gas data – We believe that the privacy considerations for gas are less than for electricity, as gas consumption data is less revealing about consumer lifestyles. Security risk (for example a cessation in gas consumption in the winter may indicate absence from the property) could be minimised but reduced access to very recent consumption.



Access by suppliers to sub-daily data – Whilst gas meters can measure at high frequency such as half hourly, this functionality is not used at present for billing and settlement purposes. We do not think that regulation now should preclude development.

Question 3: Do you support the proposal to develop a privacy charter?

- Yes, with reservations
- We believe that the Data Protection Act is sufficient and clear
- We will support the development of the privacy charter, and expect to sign up to it, strictly subject to leadership and support from the Information Commissioner's Office, and its function being limited to contextualisation of the Data Protection Act

Question 4: What issues should be covered in a privacy charter?

- The privacy charter should not go beyond the Data Protection Act

The Data Protection Act - we strongly believe that the privacy charter should contextualise the Data Protection Act (and possibly the European Convention on Human Rights Article 8), but should not go beyond it. If the Data Protection Act is insufficient or needs changing then this should be done directly within the Act and the associated processes for primary legislation, secondary legislation and the issuance of guidance.

Privacy regulation - It would be wholly inappropriate to have any Personal Data Protection requirement that is governed other than by the Act (and other relevant legislation such as the Freedom of Information Act and the Environmental Protection Act).

Question 5: Do you agree with our approach for ensuring the end-to-end smart metering system is appropriately secure?

- Yes, broadly, although more consideration needs to be given to the interim period
- We draw greater distinction between privacy and security
- We believe that more needs to go on HAN security

Interim period – We have a number of reservations about the interim period between smart meter mandation and DCC go live. One interim solution is an interim central service provider (which we would support as it mitigates other risks in the interim). However this solution, and other solutions where there are systemic security risks, requires a detailed work through to determine and solve security risks. The importance of consumer buy-in and stakeholder interest in matters of security and privacy can hardly be overestimated. The interim period may be inherently less secure than the post DCC go-live period and early issues arising will require rapid solution.

Privacy and security -We have noted that there may be a trade-off between privacy and security. For example, if a customer has a high degree of configurations with which to authorise data access (e.g. morning power consumption to party A, B and C, weekly gas consumption to D, E and F), then there is a high data and processing requirement and encryption and complex exchange of keys. To keep the data carriage, storage, processing and governance/audit cost manageable does require limits to configuration or security.



We believe that security protection should be as absolute as possible, and that it should not be compromised by considerations of privacy that are not essential. A good security system will give the best protection of privacy.

HAN – we believe that the HAN security needs further work, particularly if the IHD will communicate two way

