21st November, 2011

Smart Metering Implementation Programme: a consultation on the detailed policy design of the regulatory and commercial framework for DCC

Dear DCC Licensing Team,

As an electricity consumer, I would like to provide a response to the above consultation document to express my concerns about some of the implementation details.

My greatest concern is the security of the smart metering system and its ability to withstand intrusion. The proposed requirement for WAN (Wide Area Network) connectivity in chapter 6 means that smart meters will be accessible to outside groups (even without Internet connectivity, due to security weaknesses in utility company networks) and therefore almost surely subject to compromise. Since this infrastructure will be in place for 10-20 years, future attack vectors need to be considered also, including the ability to decrypt and manipulate 3G transmissions.

As such, it is critical to consider the scope for abuse with each of the message types proposed in table 6.1(pages 91-92) and to reconsider certain features.

Remote Dis/Enablement of Supply

This poses two risks- it allows companies to bypass existing control mechanisms (specifically the courts to gain forced entry to an address) and fast-track disconnections. It also opens the possibility of third parties sabotaging the gas/electricity networks by disabling supply for large numbers of domestic users, or a smaller number of industry users.

By using the Security/Software Patch message, an attacker could additionally corrupt the meter firmware, disabling it after shutting off supply. Correcting this would then require wide scale meter replacement (taking weeks or months) and could result in the deaths of thousands during cold weather.

Addressing this should therefore be considered as a matter of national security.

Even without the software patch option, sending sequences of on/off messages could result in damage to consumer and supplier equipment.

Removing this facility altogether would be the safest option. Less secure alternatives include:

- having the meter ignore enable/disable messages for a period of time (15-30 minutes) after processing one, in order to prevent the on/off scenario mentioned above.
- requring multiple disable messages from different sources (e.g. from the supplier and the DCC) before switching off supply.
- providing smart meters with a second "high priority" connection for critical circuits- this would not be affected by disable signals but would be restricted to a lower current (say 10 amps, compared to the 100 amps limit for most households). Disabling supply would then cause severe inconvenience to consumers without cutting them off completely.

Reduce loads and Switch on/off options (EV chargers, heat pumps, etc).

While not as critical as "supply disablement", these messages can be abused (disabling EV chargers when electric vehicle use is widespread would have significant economic impact). In addition, how such features would work (the smart meter cannot alter consumption of any device connected via a consumer unit) needs consideration at an early stage (possible options include separate connections for such circuits on the meter, intergrating the meter with the consumer unit or using wireless connectivity to communicate with the devices or their power sockets).

To Limit abuse of these messages, an override switch for each option should be included on the meter. This switch would self-reset (afte
critical items (e.g. EV charging could justifiably be considered critical for a doctor or emergency services worker). The use of such overrides would be noted by the meter and could incur an extra charge from the supplier.

Gas Calorific Valuetfariff Update

Malicious use of this could include sending artificially high or low values, resulting in incorrect billing. If meters instead include the time of consu mption (e.g. a list of units used per half-hour) then tariff calculations can be performed on the suppliers' systems.

Electricity/Gas/Water Meter Read (both scheduled and on demand)

The risk here is more of privacy than security - as such, measures should be considered to hinder unauthorised data collection. Options include:

- using asymmetric (public/private key) encryption to both protect data in transit and to verify the intended destination (needs public key verification when installing meter- meter will require keypad and alphanumeric display).
- keeping meter numbers and information sent via the WAN separate from account holder details. Meter details should instead be linked to an address identifier which could then only be linked to a bill payer by the supplier contracted for that address.
- the frequency of scheduled meter readings (48/day) seems unnecessarily high. As long as meters note the time/day of consumption (e.g. providing an hour-by-hour list) then a daily or weekly read should suffice, while allowing scope for numerous off-peak tariffs. This would increase message size, but lower the number. Meters would require an internal clock, which could be calibrated via the MSF radio signal or via a "time-synch" message.
- 100% coverage will not be achievable (due to adverse reception areas, such as basements or addresses not reachable by 3G) so provision needs to be made for offline reading- one option is for meters with enough internal non-volatile memory (e.g. flash memory) to store usage and diagnostic data for several months. This could be transferred onto a USB stick (or similar device) by a meter reader, or even the user (if the data is encrypted to prevent tampering) and sent to the supplier for analysis and processing.

Responses to the consultation questions follow - but I do wish to again highlight my concerns at possible abuse of the smart meter system as proposed. It is unrealistic to expect the DCC customers (or the DCC itself) to be able to maintain a completely secure network, so steps need to be considered to limit the damage that a security breach could cause.

Consulation Question Responses

1 There needs to be a clear definition of a "smart meter" to clarify the situation with meters used by private generators (including domestic wind/solar energy producers with export and feed-in tariff meters).
2 Companies that offered "free" solar panels to homeowners (where the company receives the feed-in tariff) typically monitor the performance of their installations remotely (in effect, providing their own smart metering) - this needs to be considered in prohibition legislation.
3-13 No comment.
14 Smart meters can provide usage information but only if features like displays and wireless data transmission (to allow users to view their consumption around the house) are included, at extra cost. If the purpose of smart metering is to lower consumption, this should be included as an obligation to ensure that meters are appropriately equipped.
15 No comment.
16 Objective (g) (maintaining data security and privacy) is a requirement that has to be considered at the outset- I have raised specific concerns over the possible abuse of certain message types previously- see above.
17 No comment.
18 Energy networks should remain the responsibility of the appropriate Distribution Network Operator (DNO)- where the DCC can identify issues (e.g. persistent over- or undervoltage) it should have the role of aggregating and reporting information to the DNO for further action.
19 See response to question 14 above.
20 I agree with the definitions proposed, but would suggest that the "wholly unrelated" services should also require Authority consent.
21 Some meters will not be WAN-accessible- see comments on the Meter Read message type above. Would such meters be considered non-compliant?
22 No comment.
23 Users should be informed (and their consent required) of any service making use of their personal data, notably their usage record. Users should be informed (without needing consent) of services making use of non-personal data (e.g. "electricity quality measurements", aggregate consumption of a neighbourhood, etc).
24 Having standard terms and conditions laid out in the SEC and referred to in subsequent bilateral agreements would provide consistency and enforceability.
25 No comment.
26 Given the critical role that smart meters will have in the UK's energy infrastructure, extraordinary care must be taken over their selection - not least to avoid the possibility of back doors included in their firmware. Having such firmware produced in-house (or provided by someone other than the meter manufacturer) would increase costs but could provide better security, as would making it open source. Clear guidance needs to be included in the SEC as to what extent security (and privacy) should take priority over cost.
27 Security is conspicuous in its absence from the requirements listed.
28-30 No comment.
31 Specific provision may be needed in respect of suppliers which, by nature of their customer base (e.g. more prepay meters) or supply choices (e.g. heavier reliance on variable renewable sources) impose a heavier cost on the DCC. Since these are likely to be smaller suppliers (e.g. Ebico, Ecotricity) giving such (with fewer than 50,000 domestic customers- the same level set for compulsory Feed-In Tariff payments) greater protection may be a useful compromise.
32 Independence from suppliers would seem critical given that DCC may have a role in arbitrating disputes over usage.
33 20% (the level proposed for "competitive environment" users) seems a reasonable maximum to apply generally.
34 Yes to all questions.
35 No comment.
36 Yes to both questions- though exceptions should be available for non-licensed activity in the public interest (e.g. providing usage data to National Grid to help forecast future demand)
37 The provisions would seem appropriate for inclusion in DCC's license.
38 If flexibility is to be allowed, the financial security provided should be subject to periodic review.
39 This would depend on the degree of fault that lay with the DCC- licence revocation due to reasons outside

its control should not incur extra costs.

40-41 No comment.

42 No- such a task would be better left to an industry regulator. At worst, it could lead to conflicts of interest in DCC's dealings with service providers.

43 Assuming that 3C services are being used for WAN connectivity, the ability to port numbers (transferring smart meters to another 3G network without requiring a change of phone number or SJM card) would seem critical.

44 Ten years seems overly long, particularly for a new organisation able to define the playing field for all future contenders. A shorter "rolling contract" applicable for up to 10 years, followed by fixed term contracts could offer a better balance Qf accountability.

45 See previous answer.

46 Forecasts made on licence application are unlikely to be accurate- a forecast submitted shortly (say 6 months to 1 year) before the end of the contract term would be more reliable, when the DCC has years' experience of running costs to draw upon.

47 Yes, and should be held accountable for any financial penalties in failing to do so.

48 Transfer of staff and related items (pensions, employee benefits) need consideration.

49 Yes.

50 Such an approach would make forecasting cost difficult- this would likely be a major disincentive to potential DCC applicants.

51 It would seem most appropriate for the DCC's registration obligation to parallel the smart meter rollout- i.e. once an address receives a smart meter, it is then registered with the DCC.

52 Yes.

53 Yes.

54 For domestic consumers, it would be best to allow the existing regulators (the Energy Ombudsman or OFGEM) to handle arbitration. For DCC service providers and DCC users, an independent arbitration panel should be offered with the option of intervention by the Secretary of State in matters of national interest.

55 This may not be desireable- it could interfere with "green energy" tariffs and their suppliers (e.g. Ecotricity).

56 If the DCC is responsible for supplying the meters, it should be encouraged to provide tamper-resistant and resilient ones- so it should bear secondary responsibility for theft/damage (i.e. only obliged if the individuals responsible cannot be traced). Carbon footprint reporting should only be considered within the framework of a more general environmental impact assessment.

57-61 No comment.

62 Security, including thhd party assessment ("penetration testing") and the possible need of urgent updates to correct any critical flaws identified in the DCC network.

63-72 No comment.

73 Yes- but there may be an argument for allowing extra charges for meters with extra functionality (e.g. higher quality displays, wireless monitoring, extra circuit controls, etc).

74 No comment.

75 Yes.

76 This would contradict the "non-discriminatory" provisions of section 3.191 (question 55).

77-78 No comment.

79 Subject to this being possible/practical to administer, yes.

80 See initial notes regarding meter read frequency. Traffic should be encrypted and this will increase message size considerably, so it would seem more desirable to have fewer larger messages. This would require meters to collect consumption data at regular (say half-hourly) intervals and to send that data, with the times, once per day (the send time should be random but consistent- perhaps based on the meter registration number- in order to spread communications traffic throughout the day).

81 No comment.

82 Since tariffs will depend on the supplier, it would be simpler (and safer, as noted above) to exclude tariff update (and gas calorific) message types. Suppliers can calculate the appropriate values from the consumption/time figures supplied by the meter.

83-104 No comment.