SP ENERGY NETWORKS

Regulation & Commercial

By e-mail

Smart Metering Implementation
Programme
Department of Energy & Climate Change
3 Whitehall Place
London
SW1A 2AW

Your ref

Our Ref

Date
25th August 2014

Dear Colleague

A Consultation on New Smart Energy Code Content (Stage 4)

I am writing on behalf of SP Energy Networks in response to the above consultation paper issued on 30th June 2014. We welcome the opportunity to comment on the points raised.

I hope that this response is helpful, but please contact me if there are any queries

Yours sincerely

Ochil House, 10 Technology Avenue, Hamilton International Technology Park, Blantyre, G72 0HT

Telephone: 0141 614 0008

www.scottishpower.com

A Consultation on New Smart Energy Code Content (Stage 4)
Detailed comments by SP Energy Networks, August 2014

Question 15: Do you agree with the legal drafting in relation to Security Governance?

We understand CESG have made much of the shortcomings of Common Criteria (ISO15408), positioning CPA as a more rigorous standard to meet exacting UK requirements. We therefore suggest the SSC role should be to do no more than propose changes to the Security Characteristics.

Q15a: Do you agree with the Governments proposals in relation to Security Assurance?

We agree with the basic premise of having a standardised approach to assurance testing, but have some reservations around extending the role of the Competent Independent Organisation (CIO) to the Service User organisations. The qualifications for the CIO are heavily weighted towards HMG Information Assurance methods and standards (requiring CHECK registration and the employment of CLAS consultants for example) but the Service Users are not required to follow these methods and standards, nor will they necessarily have access to either the documentation or expertise to judge their readiness.

We strongly support the notion that CIO assessment activities will rely upon existing certification (e.g. ISO27001) but would be keen to see that more codified, in terms of what the impact on assessment activities would be and what level of evidence would be required.

Q16: Do you agree with our proposed approach and legal text for SEC in relation to Privacy Assessments?

Whilst we agree that privacy compliance auditing is a good thing, we do not agree that there is a strong parallel between security and privacy compliance. The risks are very different, reflecting the different focus. We also disagree that there is much synergy between ISO27001 and the Data Protection Act 1998 when it comes to requirements. There is a compliance assessment for DPA defined in the ICO's Privacy Impact Assessment handbook v2.0. These factors contribute to our strong reservations about a joint audit:

- assuming a security "auditor" from the CIO will be a CLAS consultant, this confers no significant qualification to consider privacy except in the most general terms.
- there is nothing (so far as we are aware) in the qualification requirements for a CIO that requires suitably qualified privacy practitioners (BCS, Law Society or CIPP/E)
- we believe there is some synergy to be had in running the two audits in parallel (joint planning and wash up meetings etc. and possibly a single final report) but we believe it requires two separate auditors.

Q18: Do you agree with the proposal for Users to meet the costs of the privacy assessments that are undertaken at their organisation?

Yes, we fully concur that this is the simplest and fairest approach to charging.

Q19: What are your views on potential future changes to the SEC to provide for reporting the results of privacy assurance assessments bodies such as Ofgem, DECC, ICO and Parties generally?

Whilst reporting the results of privacy compliance assessments is generally a good thing, it should be noted that wide distribution of these reports could provide a basis for a range of stakeholders to make a Request for Assessment, leading to the ICO issuing Information Notices and possibly Enforcement Notices against the User organisation.

Q26: Do you agree with the proposed approach for all Network Parties to have established SMKI Organisation certificates?

Whilst we fully understand the logic behind obliging a DNO to register for organisation certificates before enrolling as a DCC User, we believe that there are substantial risks in the proposal for the DCC to hold the keys:

- There is a risk of loss of the private key when it is eventually transferred to the DNO for import into their HSM(s). This needs to be mitigated through a key splitting algorithm. This causes some degree of complexity in the logistics of transporting the keymat to the DNO and also requires that both the DCC (or whoever holds the keymat) and the DNO have operational and compatible key management suites supporting whatever key splitting algorithm is selected.
- There is a risk of exposure of the keymat during transfer, which needs to be mitigated through appropriate encrypted storage media.
- Finally, since the private key will have been held by someone other than the DNO, we believe this may cause a serious problem for the trust model and hence for legal liability. An alternative approach would be to have some form of key escrow agreement between a DNO that elects to generate their keys and certificate before enrolment and a suitable 3rd party, perhaps the SMKI service.

Question 32: Do you agree with the intention to create a 'Party ID', enabling access to the Self Service Interface at a Party level?

We believe the creation of the party ID is overly complex and can be avoided by SECAS recording which party has requested a particular ID

Question 44: Do you agree that Network Parties using the same RDP should be jointly and severally liable for failure of that RDP to comply with provisions relating to the RDP's use of the connection provided to it by the DCC?

We do not agree that network parties should be jointly and severally liable for failure of a shared RDP service. Our preference would be for RDP agents to become SEC parties (as Supplier Agents are) and would therefore have obligations under the SEC in their own capacity.

Question 56: Do you agree with the proposed approach and legal drafting regarding power outage alerts?

Whilst we approve the inclusion of the requirement to provide power outage alerts explicitly within the SEC a large amount of uncertainty will still remain around the provision of this information. For example, when used operationally this information will have a time critical nature which is not covered here. In addition, the implication in the consultation that filtering should be applied by the DCC raises issues around how this filtering could be intelligently applied without knowledge of our network i.e. 50 messages across our whole network at one point in time might tell us almost nothing, 50 messages in relation to a single incident may be fully adequate for our needs.

Question 57: Do you agree with the proposed approach and legal drafting in relation to the testing of shared systems?

- We fully support this approach as being the optimal use of resources
- We would expect the same approach to apply to RDP connections.

Question 58: Do you consider the costs of remote access to the test SMWAN should be socialised across all Users or charged directly to those test participants who use the service? Please provide an explanation for your answer.

We believe access to the test SMWAN should be charged directly to participants who use the service. We believe the level of testing will be skewed to a subset of user roles and it would be unfair to socialise these costs. In addition, we believe direct charges will deter spurious testing of immature devices.