Dear Madam, Sir,

Please find our answers to the: "Smart Metering Implementation Programme: Consultation on the second version of the Smart Metering Equipment Technical Specifications (URN 12D/258)".

If any of those is not clear or complete enough, please don't hesitate to contact me for further information.

I have concentrated my answers on the topics related to data security and privacy.

Regards,

2. Do you agree with the proposal to adopt ZigBee SEP / DLMS as the HAN application layer standards for GB?

Yes but we would add an additional requirement making mandatory the activation of the security mechanism of the chosen application layers.
We would also recommend to make clear which DLMS/COSEM is selected: the current one of the new one that will be standardized in 2013 (i.e. the new one among others introduces a new security profile where ECC crypto is used instead of AES in GCM mode).

3. Do you agree that equipment should be required to comply with SMETS and a GB Companion specification for ZigBee SEP / DLMS?

Yes

21. If DNOs were permitted to access remote disablement functions, should control logic be built into DCC systems or meters? If the logic should be built into meters, should the logic be specified in SMETS 2? Please provide rationale to support your position including estimates of the cost of delivering this functionality under the different options being considered and any evidence relating to safety issues associated with each option.

We would recommend to add the control logic in both the DCC and the meters for security reasons (i.e. we are not addressing the safety issue here). Security should be handled end-to-end and if one line of defense fails there should be another one to withhold attacks.

22. Do you agree that variant smart electricity meters should be specified in SMETS 2 and that the cost uplift for variant smart meters is similar to that for variant traditional meters? Please provide evidence of costs to support your views on cost uplifts.

Yes for security reasons, any device connected to the DCC should be equally covered by SMETS2.

23. Do you agree that randomization offset capability should be included for auxiliary load control switches and registers as described above? Do you have views on the proposed range of the randomization offset (i.e. 0 – 1799 seconds)? Please provide evidence on the cost of introducing this functionality.

Yes and for security reasons the randomization should be really random and the random generation should be securely performed (i.e. the implementation should be tamper resistant against local and remote attacks).

24. Do you support Option 1 or Option 2 for 'pairing' a CAD to the HAN? Please present the rationale for your choice and your views on the implications that these options have for the technical design of the solution.

We would also recommend to investigate the feasibility and security of NFC pairing that are known to be far much more user friendly and by the physical proximity also privacy preserving.

26. Do you consider that other CAD installation options should be pursued? If yes, please explain the approach you favor and your reasons.

Yes as stated in answer to question 24, we think that NFC pairing solutions should be investigated as well.

27. Do you agree with the proposal to include in SMETS 2 a specification for a PPMID, connected via the HAN, as described above?

Yes and for this one we would also recommend to investigate whether a NFC solution could be more appropriate and more user friendly.

29. Do you agree with the proposal that the communications hub should be specified such that it can support multiple smart electricity meters? How many smart electricity meters should be supported by each communications hub?

Yes.

30. Do you agree that a specification for a HHT interface to the HAN should be defined? If yes, please identify the functions that this interface would need to support and the scenarios in which such functionality could be required.

Once again we would recommend to investigate the use of NFC for the HHT or maintenance interfaces.

31. Do you agree with the proposed approach to the governance of security requirements? If you propose alternative arrangements please provide evidence to support your views.

Yes and no. Security is kern to the success or failure of the Smart Grid concept. Our perception is that in the current proposal, the security requirements are not directive enough. This is an exception where you should not let the market decide but where the government should decide for the good sake of the national infrastructures.

There exist only a few schemes in the world of security that get general recognition and that survived the last years: Common Criteria and FIPS certification.

32. Do you agree with the proposal to establish independent assurance procedures

for DCC and DCC users? Please explain your views and provide evidence, including cost estimates where applicable, to support your position. Comments would also be welcome in relation to the impacts and benefits of the proposed approach with regard to small suppliers.

Yes. Experience has shown that the domains where security is successful are the domains where state of the art and well proven assurance procedures are mandatory.

33. Do you agree with the proposal that re-testing should occur at least at set intervals and more frequently when significant changes to systems or security requirements are introduced? Please explain your views.

Yes. Experience has shown in Common Criteria (see the work of the JHAS group) that attacks evolves with time and that a device that gets a certificate at one give point of time may not be able to get the same certification level one or two years afterwards.

34. Do you agree with the proposal to establish an independent security certification scheme for smart metering equipment? Do you have any views on the proposed approach to establishing a certification scheme or evidence of the costs or timelines for setting up such a scheme or submitting products for certification?

Yes. We would recommend to team up at the European level for the definition of a Common Criteria protection profile for each kind of devices (meter, communication hub...) and to reuse the Common Criteria independent procedures, evaluators, labs...
Germany can be used as a template but it should be preferably adapted to get European wide or even better worldwide (to favor broader interoperable markets) acceptance.