www.ipso-alliance.org

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

Re: Consultation on the second version of the Smart Metering Equipment Technical Specification
Consultation reference: URN 12D/258

Dear Sirs,

We have reviewed the document "Consultation on the second version of the Smart Metering Equipment Technical Specification" dated 13 August 2012 and have some serious concerns over a few of the proposed recommendations most specifically related to the adoption of Zigbee SEPv1. We feel that this choice will lead to significant problems related to interoperability, management, scalability, security and future enhancements. As such we would recommend that the Smart Metering Implementation Programme re-evaluate your decision for SMETS v2 of using SEPv1.

The IPSO Alliance is an open multinational business alliance of over 60 companies that work to promote the use of the Internet Protocol (IP) in embedded networking applications such as those used in Machine to Machine (M2M), Industrial Control, Building and Home automation, Healthcare, Automotive and of course the Smart Grid and Smart Energy. The IPSO Alliance does not attempt to define protocol specifications but instead works with Standards Developing Organizations (SDOs) such as IEC, ITU, IETF, ANSI and others. We work with these groups to identify gaps and to promote their open standards works. We have worked diligently with U.S. Utilities, the U.S. National Institute for Standards and Technology (NIST), the U.S. Smart Grid Interoperability Panel (SGIP) and the U.S. Department of Energy on the protocols selected to be used in the U.S. Smart Grid and in particular the Home Area Network protocols which are most closely related to your Consultation. It was during this work that we helped these various organizations recognize the limitation associated with the Zigbee SEPv1 specification and implementation and as a result NIST, the SGIP and many U.S. utilities have abandoned SEPv1 in favor of SEPv2. The SEPv2 protocol has now been adopted by the HomePlug Alliance, WiFi Alliance, and HomeGrid Forum. It was determined that there are significant interoperability and security issues related to SEPv1 and that SEPv1 is not easily interoperable with the Internet, the World Wide Web or any of the Utilities enterprise networks. Only through the use of gateways and protocol translators can

a SEPv1 network be made to work with existing systems and these gateways break network and end-to-end security, lead to management and interoperability problems, increase the overall cost of the system and cut off any future innovation.

Please see below for answers to your specific questions in the Consultation on SMETS 2. We are encouraged by the work done your department and the broad open review of your recommendations and we hope that you will find a technology that provides a truly open interoperable and secure solution that allows for innovation in Smart Energy Applications and the SMETS.

REDACTED REDACTED REDACTED
REDACTED REDACTED REDACTED
REDACTED REDACTED REDACTED

Chapter 4 Question 1 - *Do you have any comments on the criteria used in the evaluation of the application layer standards?*

The criteria as specified in the Consultation appear to be well thought out. The requirement for interoperability is particularly well founded, but it is then interesting to see the recommendation of SEPv1 which has been found to have considerable interoperability problems between different vendors that have all "completed Zigbee SEPv1 testing and certification". The requirements for security and use of open protocols are also extremely pertinent, though again we fail to see how the SEPv1 protocol that is controlled and developed within a member only organization meets the requirements of openness.

Chapter 4 Question 2 - *Do you agree with the proposal to adopt ZigBee SEP / DLMS as the HAN application layer standards for GB?*

This is the crux of our concern of the recommendation for SMETS v2. While we fully support the work of the Zigbee Alliance on SEPv2 which is based on open standard protocols as required by the SEPv2 Market Requirements Document, we have voiced our concerns about interoperability, security, certificate management, maintainability, manageability, scalability, protocol longevity, and application innovation with respect to SEPv1. We feel that SMETS v2 programme will fail to achieve its goals should the choice of SEPv1 not be reconsidered. As groups in the U.S. determined, SEPv1 fails to meet many of the basic requirements for the Home Area Network and as a result they instead chose to implement SEPv2 as now being delivered by most major meter and AMI manufacturers. The problems related to SEPv1 are systemic and cannot be fixed by patches.

As an example the network stack was designed as what is pejoratively called a 1-2-7 stack. This means that the typical and industry standard layered stack design - a stack design using the OSI Seven Layer model as called out in Paragraph 33 of this Consultation - was not used in SEPv1. Instead only layers 1, 2 and 7 of the model were implemented in SEPv1. This 1-2-7 architecture is used in many similar proprietary network specifications, but is being replaced by the more flexible and manageable complete ISO model. [It is also worth noting that the cost of the communication devices (radio modules) is not increased by switching to a more complete and standard architecture - in fact there are implementations that show that open standards IP based implementation can be smaller and therefore less costly than these proprietary 1-2-7 implementations like SEPv1.]

Choosing to ignore the decoupling provided by proper layering eliminates the

possibility to include alternative networking media. This means that should a different physical media be necessary to provide connectivity it is not possible to include it in the solution. SEPv1 cannot be used over any other communications media other than 802.15.4. It cannot be used with WiFi (802.11), or PLC (P1901.2), Ethernet, cellular, ... Therefore the requirement recognized Paragraph 35 of providing a wired HAN solution is not compatible with SEPv1. To incorporate a wired network solution will require the added cost of yet another gateway device to translate and interconnect the wireless SEPv1 network with the as yet undetermined wired network. It is extremely important to understand that the wired network will not and can not be SEPv1 since SEPv1 is inextricably tied to 802.15.4. This means that SMETS v2 solution will have to include two non-interoperable networking protocols should SEPv1 to used for the wireless network.

In addition the SEPv1 uses an Application layer that is unique to Zigbee and extremely complex and not easily compatible with the World Wide Web - as compared to SEPv2 which uses an HTTP application layer and open standard XML for data representation. Basing the application layer on these well recognized and universal standards is of paramount importance to enable easy integration of HAN capabilities and devices into the enterprise systems of utilities and alike, and is also important in order to enable innovation and time-to-market related to application development. SEPv1 does not fulfill such expectations. It should also be noted that any concerns regarding these web technologies as being too verbose in resource constrained environments is overcome by existing open standards in the IETF.

As previously mentioned SEPv1 has been shown to have both interoperability and security implementation issues that are not easily fixed. In addition SEPv1 requires the used of Gateways to translate from the Zigbee Pro networking protocol and SEPv1 application protocol into an Internet compatible protocol and application framework. These Gateways break any form of end-to-end security because the application data must be decrypted at the gateway and then re-encrypted by the gateway prior to encapsulation in the IP packet for transmission over the Internet. This provides for an extremely vulnerable attack vector where an intruder could intercept and change or insert usage data or control messages thereby rendering the network untrustworthy. This gateway also creates a single point of failure and adds significantly to the cost of the overall system. The adoption of IP in SEPv2 alleviates these issues. To compound the security problems, SEPv1 requires proprietary security technology which is no longer considered adequate by and per the recommendations of the U.S. NIST. Security Certificates are mandatory and must be purchase from single vendor. Additionally membership in the Zigbee Alliance is a requirement to be eligible to purchase these certificates.

In Paragraph 37 the Consultation requires that solution must meet the requirements

of being an open standard. SEPv1 is not a recognized open standard - though requested it has not been accepted and may not be accepted due to the closed nature of the Zigbee Alliance and intellectual property issues related to SEPv1. The UK Government and this Programme should not count on or expect that SEPv1 will ever be recognized as an open standard.

Paragraph 40 states that SEPv1 compares well against the criteria. Given the information provided above and implementation experience in the U.S. it is unclear how this could be considered accurate. While it may be construed from marketing literature from the Zigbee Alliance and SEPv1 vendors that SEPv1 provides some level of functionality required by the SMETS programme, actual implementation experience from Utilities in the U.S. has shown otherwise. Instead SEPv1 is not open, interoperable, secure or in reality mature.

Chapter 4 Question 3 - *Do you agree that equipment should be required to comply with SMETS and a GB Companion specification for ZigBee SEP / DLMS?*

Absolutely, so long as the SEP specification that is being referred to is SEPv2 and not SEPv1.