

SMART METERING PROSPECTUS

28th OCTOBER 2010 QUESTIONS – SUMMARY RESPONSES FROM ASTRIUM.

Astrium Services is a major player in the areas of aerospace, telecommunications, and earth observation. Through its subsidiary, Paradigm Services Limited, Astrium is an established and accredited provider of highly secure, high-availability critical communications services to the UK Government.

Astrium Services herewith submits its responses to specific questions raised in Ofgem's Smart Metering Prospectus, due by 28 October 2010

Introduction

Our responses to individual questions are incorporated in this document. However there are certain key elements which underlie our responses to all questions, but especially for questions 1, 2, 8-11, and 15. These concern the need for a single-point responsibility and accountability for delivery of the successfully-operating Smart Metering **System** with all required features and certified security.

Examples where single end-to-end design control is essential include:

- i) **Open design/standards.** To accommodate multiple manufacturers' equipment there needs to be a validated design with level playing field interfaces.
- ii) **Security.** To model and verify system security there must be a single configured design under a single responsibility.
- iii) **Phased and expedited implementation.** This is only possible where a design has been created and validated to allow progressive implementation of partial functionality as equipment becomes available, while retaining full integrity of operation especially in terms of system stability and security.

The processes set out by the Prospectus do not unequivocally identify an entity to assume these responsibilities (although the role of the DCC could be interpreted this way). Without clarity in this, the overall system procurement, delivery and operation could become very difficult.

The Prospectus, as we understand it, defines a set of individual responsibilities for elements of the system, with the overall responsibility being shared under the Smart Energy Code and implemented through negotiation in the various Working Groups. Such a model can work well for the development of Standards, but is not efficient for System Engineering of a major time-limited programme involving major procurements.

We recommend the assignment of a System Design Authority having these responsibilities on behalf of the overall programme in the following areas:

- repository of agreed system technical and security requirements
- maintaining the formal system design definition
- demonstrating that the design fully meets the system requirements

- specifying the processes and criteria for system integration and acceptance, including any phased implementation

Response to Specific Questions

Question 1: Do you have any comments on the proposed minimum functional requirements and arrangements for provision of the in-home display device?

Astrium support the provisioning of the in-home display device to promote consumer awareness and therefore control of energy usage. However there is a potential issue on security. For example, it may be necessary that only the IHD unit is authenticated to receive the information and it is the only device that can decrypt the data transmission. This is one of the Security issues discussed further below, and an example of where the Security requirements need to be very clearly and strongly expressed very early.

Question 2: Do you have any comments on our overall approach to data privacy?

With the potential for multiple suppliers and equipment vendors, the issue of data security is critical if an effective and secure system design is to be achieved. Astrium strongly supports the establishment of a Security Working Group by Ofgem to deal with the important and complex issues of data privacy and security. In addition to securing the hardware and software of the devices, the HAN and WAN need to be designed to protect against hacking, eavesdropping, sniffing, denial of service, man-in-the-middle, evil twin, virus, to name just a few types, of cyber attack. The security issue associated with smart metering is further complicated by the fact that the smart meter is expected to reside in a non-secure, static location. This will potentially allow a 'hacker' physical proximity to the device as well as allow time to record and subsequently decode the encrypted messages. The issue is compounded further by the requirements for easy supplier and payment method changes. Astrium supports the establishment of the Security Working Group based on industry security experts as soon as practicable.

Question 4: Have we identified the full range of consumer protection issues related to remote disconnection and switching to prepayment?

Astrium support the new approach of prepay and contract arrangements. However, as stated in the response to question 2, the infrastructure needs to address the issue that the metering device is expected to be located in non-secure areas and could be subjected to undetected long term illicit monitoring with the aim of decoding of the security algorithms. This may imply the use of some form of anti-tamper mechanism in ideally physical or more practically, in software form.

Question 5: Do you have any comments on the proposed approach to smaller non-domestic consumers (in particular on exceptions and access to data)?

Astrium support the approach. Non-domestic consumers will be able to join once the infrastructure is established. However upon joining, we would expect non-domestic consumers to share in the cost of the infrastructure.

Question 8: Do you have any comments on the proposals that energy suppliers should be responsible for purchasing, installing and, where appropriate, maintaining all customer premises equipment?

In general, Astrium support the approach as it minimises the number of separate responsibilities. However, alternative arrangements such as ownership of the WAN module by the WAN provider could also be viable, provided that equipment functionality and in particular interface requirements, are defined and standardised well in advance and that system and operational responsibilities are fully defined. The establishment of an overarching system authority (possibly within the DCC) needs to be a priority before any major roll out of smart meters and system infrastructure. Astrium believes that the HAN and WAN should be in separate 'plug and play' modules to allow separation of responsibility, maintainability and upgradability. The WAN module needs to be defined by the system design authority but maintained under direction of the energy suppliers according to the responsibilities assigned by the design authority. For example if it is decided to maintain multiple communications bearers, then responsibility for the connection to each WAN bearer may be delegated to the WAN provider. For this model to work it is possible that the WAN provider or its representative will need to gain access to customer premises,.

Question 9: Do you have any comments on the proposal that the scope of activities of the central data and communications function should be limited initially to those functions that are essential for the effective transfer of smart metering data, such as data access and scheduled data retrieval?

Astrium believe that the DCC should have the capability and be given the responsibilities for meter registration, change of supplier data transaction and translation services from day one. We see these as fundamental functions of the DCC and are necessary for the DCC to add value. Linked with this, the DCC should also be given the responsibility of making sure end to end working of data collection is fully established before the energy supplier installer leaves the customer premises. This will require a degree of coordination between the DCC and installers.

Question 10: Do you have any comments on the proposal to establish DCC as a procurement and contract management entity that will procure communications and data services competitively?

Astrium agree with the proposal, but for the DCC to perform this role efficiently and effectively, we believe the DCC needs to be assigned as the overall system design authority and be responsible for end-to-end service delivery, including WAN security and data privacy.

Question 11: Do you have any comments on the proposed approach for establishing DCC (through a licence awarded through a competitive licence application process with DCC then subject also to the new Smart Energy Code)?

Astrium support the establishing of the DCC in a competitive licence application process but we believe it vital to establish the DCC as quickly as possible early in the process. The accountability and responsibilities of the DCC must be clearly stated from the outset; it would be unreasonable and potentially costly, if this were to be delayed beyond preliminary Smart Metering roll out.

Question 12: Does the proposal that suppliers of smaller non-domestic customers should not be obliged to use DCC services but may elect to use them cause any substantive problems?

It is assumed that no part of the Smart metering system is used to transmit data from an opted out supplier/consumer. This is important from a charging and security perspective. If as can be expected, specific suppliers will supply to both non-domestic and domestic consumers, then opted out non domestic connections, must not be permitted to leak across to the secure smart metering system for domestic consumers.

If this constraint is imposed then Astrium sees no further issues other than how to incentivise opt in when a fee is likely for connect and to carry data.

Question 13: Do you agree with the proposal for a Smart Energy Code to govern the operation of smart metering?

It is essential to have good governance of the Smart metering process. It is unlikely this can be fully achieved with a Smart Energy Code alone. The code will define the disciplines and regulation of Smart Metering but the need for single point overall

system responsibility is in our view, vital to ensure that day to day operations can be maintained at the Quality of Service levels expected of this approach. Further comment can only be made once the Code is defined.

Question 15: Is there anything further we need to be doing in terms of our ensuring the security of the smart metering system?

A major security issue arises in the upgradability of the security feature of the HAN and WAN attached devices. We must assume that illicit security breaches will be continually attempted; technology will always be available to help in this unfortunate activity. The remote and non secure location and static nature of the HAN devices will create significant challenges to the security design if equipment cost is to be maintained at the lowest possible level. This should be a key issue for the Security Working Group to address.