Trilliant

SMART METERING IMPLEMENTATION PROGRAMME: CONSULTATION ON DRAFT LICENCE CONDITIONS AND TECHNICAL SPECIFICATIONS FOR THE ROLL-OUT OF GAS AND ELECTRICITY SMART METERING EQUIPMENT (AUGUST 2011) RESPONSE TO:

Department of Energy and Climate Change (DECC)

October 13, 2011

DEPARTMENT OF ENERGY & CLIMATE CHANGE

Trilliant
1100 Island Drive • Redwood City, CA 94065 USA • +1.650.204.5050 • **www.trilliantinc.com**

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION 1.
Annex 1 – Digest of Consultation Questions

Introduction

Trilliant fully supports the Government in its vision of every home in Great Britain to be equipped with Smart Metering Equipment, with businesses and public sector users also having smart or Advanced Meters suited to their needs. As a key stakeholder in this process, Trilliant appreciates the opportunity to help shape the framework for implementing this vision. Trilliant believes that sharing our knowledge and expertise in this area will also help the Government achieve its vision.

Trilliant has responded to the questions posed where our input was felt to be most useful. The following key thoughts are addressed in response to the questions:

- An assurance framework would be counterproductive for the Foundation phase, but necessary for the enduring solution to ensure interoperability.
- The deployment of Communications Hubs will ensure the open market where the retailers can provide the services to compete without prerequisite barriers such as requiring an electricity meter being installed prior to the gas meter.
- Trilliant recommends against the adoption of the provision for the support of a single protocol (DLMS) over the WAN as it will limit solution flexibility and increase complexity.

About Trilliant

Trilliant provides communication solutions that deliver on the benefits the Smart Grid to utilities and their customers. These benefits include enhanced energy efficiency, improved grid reliability, lower operating costs, and integration of renewable energy resources. Trilliant currently has more than 200 utility customers including Centrica, Iberdrola USA, and Hydro One Networks, and is backed by prominent investors such as ABB, GE, Investor Growth Capital, MissionPoint Capital Partners, UMC Capital, VantagePoint Venture Partners, and zouk ventures. For more information, visit **www.trilliantinc.com**.

THIS PAGE INTENTIONALLY LEFT BLANK

Trilliant Response to Annex 1 – Digest of Consultation Questions

8.	**What contribution do you think the interoperability licence condition as drafted could play in ensuring that suppliers work together to ensure Smart Metering Equipment is interoperable? Please explain your reasoning.**
	Trilliant Response: Trilliant believes these contributions are necessary but not sufficient. For the enduring solution, but not during the Foundation phase, we believe that an assurance framework is also necessary to ensure interoperability of Smart Metering Equipment. Please refer to the responses provided to questions 54 through 57.
9.	**Do you think the licence conditions as drafted effectively underpin the policy intention to ensure Smart Metering Equipment is interoperable? Please explain your reasoning?**
	Trilliant Response: The license conditions underpin the policy, but Trilliant believes that for the Enduring solution an assurance framework may be useful to ensure interoperability of Smart Metering Equipment. Please refer to the responses provided to questions 54 through 57.
10.	**What role could a dispute resolution mechanism have a role in ensuring interoperability? What key features should such a mechanism have?**
	Trilliant Response: Interoperability should include the open verification of test cases before certification as well as the use of golden units in the certification process. These steps will reduce testing disputes. Dispute resolution should be worked out as part of the assurance framework.
13.	**Do you think under the new and replacement obligation gas suppliers should be given the option to wait for the installation of electricity Smart Metering Equipment before installing the gas Smart Metering Equipment? Please explain your reasoning.**
	Trilliant Response: Trilliant believes that gas suppliers should be given the option to wait for the installation of electricity Smart Metering Equipment (SME); however, the option should also be available for the installation of gas SME prior to the installation of electricity SME. Trilliant supports a system architecture with a standalone communications hub that enables different electricity and gas meter suppliers.
14.	**Do you think there are any other barriers to gas Smart Metering Equipment being installed before electricity Smart Metering Equipment? Please explain your reasoning.**
	Trilliant Response: Trilliant supports the deployment of standalone Communications Hub powered from the power mains. In cases where gas SME is deployed prior to the electricity SME, there may not be the necessary power connector for the Communications Hub. Trilliant believes the specification should call out a way for a standalone Communications Hub to be powered prior to the deployment of electricity SME.
24.	**Do you think that there are other requirements that the Government should adopt in the SMETS? Please explain your reasoning.**
	Trilliant Response: Trilliant believes that Smart Metering presents a unique opportunity for energy retailers to create additional value for customers by offering innovative products and services through the data communications channel created as part of the SMS. In order to facilitate the offering of these services, the SMETS should define a mechanism for the extension of communication services into a home network and enabling the DCC to prorate

	the usage charges for communications that support these additional consumer services. The SMETS should also offer flexibility for retailers to offer services and capabilities beyond an IHD. The IHD features should represent minimum criteria for acceptance without restricting the functionality of the IHD. As retailers offer new services to consumers utilizing the communications channel provided by the SMS, these consumers will decide which capabilities and features provide real value and respond accordingly. Trilliant also believes that ensuring that meter data values are not modified in the SMS is a matter of good policy and will enhance the acceptance of the Smart Metering Systems by consumers. The SMETS should specify that meter data be left in its native format and that data translation should be avoided so data is delivered intact to the service provider. To support accurate time synchronization between the head end system and the hub, the WAN should support a network protocol that does not automatically retransmit messages. For example in the IP network time synchronization messages should be sent using a UDP transport mechanism and not a TCP transport mechanism.
25.	**Do you agree that all the requirements recommended in the IDTS should be adopted by the Government in the SMETS? Please explain your reasoning.**
	Trilliant Response: Trilliant recommends against the adoption of the provision for the support of a single protocol (DLMS) over the WAN. This provision is not recommended for reasons cited in Trilliant's response to question #39. These arguments are summarized in the following points: • A multi-protocol solution offers the flexibility for continued innovation and rich device support. A DLMS only solution will limit the SMS solution to functionality offered by DLMS and the limitations of that protocol. • Multiple protocols support necessary functions not supported by DLMS today, such as battery operated devices, pre-payment features, efficient and reliable connectionless meter repotting, efficient time synchronization, and other types of HAN devices. • Multiple protocol solutions require less overall complexity and less computing resources to implement. Because protocol translation is not required in the hub, this simplifies and improves the performance of the overall solution. • The multiple protocol solution has an overall lower cost because the communications hub is not required to do translation, which will increase the required memory, processing power, and complexity of the hub. • Security is improved with multiple protocols as messages are passed directly from the head end system to the end device without translation. When the communications hub does translation it is required to de-crypt or decode messages this creates potential security vulnerability. • Multiple protocol solution is better able to support a wide variety of devices, as protocols that are native and best suited to the features of the device can be supported directly without translation.
26.	**Do you agree that the security requirements recommended in the IDTS are proportionate to the level of risk that the End-to-end Smart Metering System faces? Please explain your reasoning.**
	Trilliant Response: Trilliant does not agree that the requirements meet the risk the Smart Metering System faces. The requirements focus too much on each individual home and put a large burden on the security of each individual consumer. While this will protect the single consumer this does not reflect the true risks to the overall system. While a rogue hacker could decide to attack an individual home, the more serious risk is from a professional organization or governments that will want to attack at a point where they can gain access to large amounts of data or large areas of the network. Protecting and verifying individual commands at the meter does not protect the consumer if there is a breach in the higher level systems. There should be less focus put on the failures that affect a single home and more focus put on the failures that can affect large areas of the network. The requirements need to focus on defense in depth: securing the head end system, securing the communications network, securing the transport layer, securing the application layer, authenticating network devices, and authenticating data. The requirements should also compartmentalize

	security such as not putting a lot of trust in the Communications Hub with such functions as translation of data. The SMETS also places emphasis on technology and how devices are secured. Many of today's security breaches are tied to human factors and not the failure of a device or protocol. Frequently, it is the people or the processes that guide individuals that fail. Trilliant recommends additional focus around the security processes for the Smart Metering System and the human factors related to security.
29.	**What unit manufacturing cost reduction do you think can be achieved for Smart Metering Equipment over the next 20 years? Please explain your reasoning. Please also provide any other comments (accompanied by evidence) on the estimated costs of the Smart Metering Equipment as set out in the Impact Assessment.**
	Trilliant Response: For the Communications Hub, Trilliant expects the cost reduction to be minimal (<5% per year). Communications Hub equipment will be cheapest during the broader rollout (2014-2019) when volumes are high. Volume shipments once the SMS is fully deployed will be lower and will not see the same volume discounts. It is possible that future technology developments may reduce the cost of the electronic portion of the equipment, but this is hard to predict. Backward compatibility to earlier SMETS versions may prevent the adoption of more advanced technology in the future.
30.	**Do you agree that the Government should include a requirement for a Communications Hub in the SMETS? Please explain your reasoning.**
	Trilliant Response: Trilliant agrees that a separate Communications Hub should be a requirement and strongly support the reasoning outlined in the document. Isolation of the WAN communications function from the metering function better supports the desire expressed in the document for gas first installation of smart metering equipment and the support of multiple energy retailers. In dwellings where support for multiple electric or gas meters are required, the installation, support, and maintenance of the SMS will be improved by having a separate Communications Hub. In addition, requiring a standalone Communications Hub during the foundation period will provide flexibility around how the WAN ownership evolves during the Foundation stage. Deployment of non-standalone WAN modules in the foundation period can create complexities around ownership and management of the WAN module that may become irrelevant depending on the outcome of the DCC planning. Keeping the Communications Hub external during the Foundation period will reduce the overall cost of the Foundation period deployments, and may significant reduce the risk of the DECC in the transition from the Foundation period to Enduring solution. Trilliant believes that the hardware cost savings to be offered by an integrated Communications Hub function is minimal and does not outweigh the overall benefits, including the additional programme flexibility, offered by the separate Communications Hub solution.
31.	**Do you agree with the estimated costs and benefits for outage detection and the Government proposal to require the Communications Hub to include the equipment necessary to provide electricity outage detection? Please explain your reasoning.**
	Trilliant Response: While Trilliant agrees with the benefits to consumers of outage detection, we feel that the cost impact of this feature could be 50-100% larger than the estimates cited in this document. In addition to the actual product cost there will be larger on-going maintenance costs associated with the battery functionality required to support this feature. Addition of a fairly large battery to support this feature will add to test, certification, and

	manufacturing costs in addition to the additional cost of the component. Furthermore, it is expected that loss of battery life or overall failure of the battery could increase the failure rate of the Communication Hub. These factors should be considered as well. Consideration of new overall system failures that result from outage message flooding of the network and head end system should also be considered. All of these factors should be taken into account.
32.	**Do you agree that the DCC Communication Service Providers should specify the requirements for outage detection as part of their general role in specifying the WAN technology? Please explain your reasoning**
	Trilliant Response: Trilliant agrees with this statement. The DCC Communications Service Providers (CSP) will need to ensure that their network has the reliability and throughput to handle broad outages, but also support outage detection down to the single dwelling level with high reliability. These requirements should be outlined in the service level agreements for the WAN technology provider.
33.	**Do you think that the Communications Hub should also have the functionality to send a communication to the DCC when power is restored? Please explain your reasoning.**
	Trilliant Response: Trilliant agrees with this requirement and does not see this requirement adding any additional hardware to the SMS beyond what is required to meet the existing outage requirement.
34.	**Do you agree with the Government's proposal that fully integrated electricity meters and Communications Hubs will not comply with the SMETS? Please explain your reasoning.**
	Trilliant Response: Trilliant agrees with this position. Full integration of the Communications Hub function into the electric meter creates a larger dependency on the electricity meter for the smart metering function. This creates large challenges in gas meter first installations that could either duplicate installed functionality or require the removal of existing equipment. Integrated electricity meters would also cause duplicate functionality in cases where multiple electricity meters might be configured to use a single Communications Hub. Finally, creating and supporting the business model around the fully integrated electricity meters during the foundation period will add unnecessary complexity and risk as the solution is transferred to the DCC. Please also see our response to question #30.
35.	**Do you think the Smart Metering Implementation Programme objectives would be better met by:** **a. Using the SMETS to mandate a separate Communications Hub with a fixed WAN transceiver? Or** **b. Giving suppliers flexibility over options for configuration of the Communications Hub33?** **Please explain your reasoning.**
	Trilliant Response: Trilliant believes the best approach is to mandate a separate communications Hub with a fixed WAN transceiver. This will set clear delineations of responsibilities in the market, and will create an environment that will allow for a lower-risk transition from the Foundation period to the Enduring solution for the DCC. Having a proliferation of different solutions – integrated or standalone hub; modular or fixed WAN, etc. – will create a proliferation of business processes and required inter-company agreements as customers switch suppliers and as the DCC takes over management. Minimizing this to the simple, clear, and well-defined interfaces of a standalone Communications Hub with a fixed WAN will simplify the transition for the DCC and ultimately lead to a lower-cost solution.

36.	**Do you agree there should be no restrictions on the HAN standards adopted by suppliers, provided they are available as a European (CEN, CENELEC or ETSI) or International (IEC or ISO) standard? Please provide evidence to support your position.**
	Trilliant Response: Trilliant recommends more specific evaluation criteria to narrow down the number of possible HAN transport standards used during the foundation period. An appendix for HAN evaluation criteria is included in the IDTS and should be used to guide the selection of HAN transport standards during the evaluation phase.
37.	**The IDTS has recommended that all standards should be recognised or be in the process of being recognised by 31 December 2014; do you agree with this recommendation? Please explain your reasoning.**
	Trilliant Response: Yes. The system should be based on open standards, and a deadline of 31 December 2014 is reasonable.
38.	**Do you think that regulatory obligations are needed to underpin a systematic approach to testing of HAN standards during the Foundation phase? Please explain your reasoning.**
	Trilliant Response: No. Robust deployments during the Foundation period will be the best possible test of HAN solutions, so regulatory effort should be focused on supporting these robust deployments. The best performing and most applicable solutions will win in the marketplace directly.
39.	**Do you agree with industry's recommendation that DLMS should be adopted as the application layer for communications with the DCC? Do you believe there are any consumer, economic or technical issues with this solution which could be circumvented by an alternative approach? Do you have any economic, technical or consumer evidence to assist Government in evaluating industry's proposal?**
	Trilliant Response: Trilliant does not agree that DLMS should be adopted as the only application layer for communications with the DCC. Trilliant does not believe that the overall industry agrees with the DLMS-only approach, and has outlined our arguments against a single application layer protocol in the Open, Multi-Protocol Communication Solution for the UK Smart Metering Implementation Program white paper provided as an attachment in Section 2 of this response document. To summarize the arguments made in the attached white paper: • A dual-protocol solution offers the flexibility for continued innovation and rich device support. A DLMS only solution will limit the SMS solution to functionality offered by DLMS and the limitations of that protocol. • The dual-protocol solution supports necessary functions not supported by DLMS today, such as battery operated devices, pre-payment features, efficient and reliable connectionless meter repotting, efficient time synchronization, and other types of HAN devices. • The dual-protocol solution requires less overall complexity and less computing resources to implement. Because protocol translation is not required in the hub, this simplifies and improves the performance of the overall solution. • The dual-protocol solution has an overall lower cost because the communications hub is not required to do translation, which will increase the required memory, processing power, and complexity of the hub. • Security is improved with the dual-protocol solution as messages are passed directly from the head end system to the end device without translation. When the communications hub does translation, it is required to de-crypt or decode messages this creates a potential security vulnerability.

	• The dual-protocol solution is better able to support a wide variety of devices, as protocols that are native and best suited to the features of the device can be supported directly without translation.
40.	**Do you agree with industry's recommendation that DLMS and Zigbee SEP 1.x should be adopted as the application layer for communications within the consumer premises, provided they install the necessary translation equipment? Do you believe there are any consumer, economic or technical issues with this solution which could be resolved by an alternative approach? Do you have any economic, technical or consumer evidence to assist Government in evaluating industry's proposal?**
	Trilliant Response: Trilliant agrees that DLMS is a recognized standard and well suited to the support of electric metering applications, while ZigBee SEP 1.x offers the capabilities needed to support sleepy gas meters as well as other elements of the SMS HAN like IHUs. As stated earlier in question #39, Trilliant does not agree that translation equipment should be part of the hub, but native communication with the devices via the WAN and HAN is preferable, even in the event this requires support of multiple application layer standards by the DCC.
41.	**Do you think the Smart Metering Implementation Programme objectives would be best met by the proposed approach above? Or should a single, network-layer technology standard such as IPv6 be mandated? Please explain your reasoning.**
	Trilliant Response: IP-based systems are available today and are considered very mature and robust. As the most widely adopted network layer addressing standard it is the most viable candidate for the SMS. It is not necessary to mandate IPv6 as a technology since there are no features of the IDTS that require IPv6 addressing. It is recommended that Ipv4 be allowed since many network providers still use it exclusively.
42.	**Is the provision of a single network-layer address for each Communications Hub a reasonable and sufficient functional requirement for the Smart Meter WAN? Will this requirement limit potential future capability or present challenges, for example, in multi-occupancy buildings?**
	Trilliant Response: Trilliant believes that a single network layer address is sufficient for the communications hub. As an intelligent network device, the hub can communicate with the head-end system via a single network address while providing services to the individual HAN devices via another protocol (such as ZigBee) that can use a different addressing protocol. End-to-end support for a single network layer addressing scheme is not required.
46.	**Do you agree with the proposed approach for consumers to access data and transfer it from the HAN via a separate "bridging" device? Please explain your reasoning.**
	Trilliant Response: Yes. Trilliant agrees and supports the bridging device outlined as option A. This configuration offers suppliers the most flexibility in terms of the protocols and devices supported for the HAN inside the home, but will lock the bridging device to one standard on the SMS side to allow for consistency across SMS devices when a change of supplier occurs.
48.	**Do you agree with industry's proposals for an overall architecture of an application layer standard with translation through a Communications Hub to a HAN? Do you believe there are any consumer, economic or technical issues**
	Trilliant Response: No. Trilliant disagrees with a single application layer standard for communication with HAN devices. SSWG and other industry groups have also voiced concern about this approach.

	Trilliant has outlined our position on the positive benefits of a multi-protocol communication scheme in a white paper that has been included in our response to question #39. As discussed in this white paper, we see significant issues related to the additional complexity, resource requirements, security features, and cost of doing protocol translation on the communications hub. This is not the approach that will lead to a robust and secure solution that offers the ability for continued innovation.
49.	**Where do you believe that translation is best managed:** **a) At the Communications Hub; Or** **b) At the DCC?** **Do you have any economic, technical or consumer evidence to assist Government in evaluating the options?**
	Trilliant Response: Translation should be minimized in the SMS. As outlined in our response to items #39 and #48, protocol and data value translation has several negative consequences and a multiprotocol solution that allows for end-to-end communication without translation will offer better performance and security while reducing overall cost. Any necessary translation should be performed at the DCC where computing resources are more readily available and updates are more easily made vs. the millions of communications hub devices that will have more limited resources and will need to be updated individually to support translation for new HAN devices.
54.	**Do you think that an assurance framework, underpinned by regulatory obligations, is needed to support the delivery of the required functionality, interconnectivity, interoperability, and security of Smart Metering Equipment? Please explain your reasoning.**
	Trilliant Response: Trilliant believes an assurance framework should not be used during the Foundation period, but would be useful for the Enduring solution. During the Foundation period, an assurance framework is counterproductive: • **Foundation assurance will slow deployment.** The standards to be used during the Foundation period have not been fully developed, and interoperability testing is not fully defined. Imposing an assurance framework at this point would create too much risk for suppliers, which would cause them to slow down their smart metering programmes. • **Interoperability will develop naturally in the market.** The market will drive a variety of compliant, but not necessarily interoperable, solutions into the market during the Foundation phase. As the standards mature interoperability testing will evolve because it is in the best interests of the market players, and an assurance framework for the Enduring solution can build on the market-driven interoperability testing. For the Enduring solution, an assurance framework can reduce the risk of incompatible variants of equipment and can increase the confidence of both retailers and customers. This confidence is important for retailers when making decisions about what equipment to deploy, especially if offered by new or unfamiliar entrants to the space. The same argument applies when new firmware versions or equipment revisions are offered by existing suppliers.
55.	**Do you agree that as part of any assurance framework adopted, there should be a testing regime in place to support the delivery of the required functionality, interoperability and security? Please explain your reasoning**
	Trilliant Response: Trilliant agrees with the use of a testing regime for the assurance framework for the Enduring solution only. During the Foundation period, a mandated testing regime or assurance framework will significantly slow down

	the deployment, and prevent market-led solutions. In general, Trilliant finds that just conformance with the specification alone is insufficient to verify interoperability with other devices, especially with newly developed standards. It is possible for two devices to be in conformance with the standard and even interoperate with a standard test device, but have interoperability issues with each other. Given the critical nature of security to the SMS, testing to ensure the functionality and interoperability of security is a necessity if consumer and retailer confidence is to be gained.
56.	**What are your views on the options outlined for a testing regime? Are there other options that should be considered?**
	Trilliant Response: Trilliant believes that each of these approaches has merit and should be considered at different phases of the program. The market-led approach is greatly preferable during the initial foundation phase of the program. During this phase, standards and industry codes are under development and new exception cases may be found that require the modification of existing standards. During this phase the necessary codes and standards may not be in place to administer a complete program governed by an independent third party. As the program matures and codes and standards are adopted and implemented, a strong testing regime with some sort of certification or accreditation is recommended. If one of the goals of this program is to build supplier and consumer confidence, then a strong test and certification program must be considered. It should be noted that this approach is consistent with industry practice today and is highly effective. Trilliant does agree with the statement that proportionality is important. The requirements cannot be so burdensome that it will discourage development of products by new market entrants and innovation for new products.
57.	**Do you think that a different approach to assurance is necessary for the Foundation and enduring phases? Please explain your answer.**
	Trilliant Response: Yes. As stated in the response to #54, 55, and 56, Trilliant believes there should not be an assurance framework during Foundation phase, but rather a market-led approach is necessary. Standards should be allowed to evolve to meet real world and real market needs. Instituting an assurance framework during the Foundation period would unnecessarily squelch innovation and significantly slow smart metering deployments. In addition, a market-led approach will enable product development teams from different companies to gather and perform interoperability tests. This approach is a proven method in the development and deployment of new technologies as they strive to reach maturity.
58.	**Do you think that the activities outlined above are a suitable way for achieving interoperability across Smart Metering Equipment cryptographic functionality? How else could this be achieved?**
	Trilliant Response: Trilliant agrees that developing an end-to-end trust hierarchy and cryptographic key management while determining how the cryptographic functions can be implemented is a suitable path to interoperability.
59.	**Do you agree that cryptographic/ key management is necessary to secure the End-to-end Smart Metering System? Please explain your reasoning**
	Trilliant Response: Yes. Trilliant agrees that cryptographic/key management is critical for end-to-end Smart Metering security. As part of the energy infrastructure, the Smart Metering System will be prime target for attack and one of the many security systems that are required to protect against the attack is a cryptographic/key management system. As has been seen with security incidents such as the one that happened with the Sony PlayStation network, an improperly managed cryptographic system can lead to a total system shut down.

	Also a proper cryptographic/key management system is required to ensure the security of personal data. Some level of personal data will be transmitted and this data needs to be secured using proper keys. Trilliant also believes that the system should be built around certificates and ephemeral systematic keys. Trilliant does not recommend that symmetric keys that are administered by master keys be used because of the key management problems that arise from weak security and large number of keys needed.
60.	**Do you agree with the Government's assessment of the advantages and disadvantages of the cryptographic solutions identified above? What other options should the Government consider? Please explain your reasoning**
	Trilliant Response: This assessment does not capture all of the different aspects of the advantages and disadvantages of the cryptographic solutions. A significant disadvantage of the symmetric keys is the management of the large number of keys which is an advantage of asymmetric PKI systems. Management of large number of keys could also be a disadvantage to the hybrid system. There is also an additional risk with a symmetric key based system where all private keys will need to be stored in a single location. In an asymmetric system the private information is stored on the device so there is no one place to get all of the private information. This eliminates a single point of attack with a symmetric system that could comprise security for all devices. To respond to the comment concerning the establishment of a Certificate Authority (CA) and the additional cost required, we would like to point out that creating a highly secure key storage mechanism for symmetric keys could end up being very costly to implement.
61.	**Do you think that it would be appropriate for the DCC to be responsible for cryptographic key management for the End-to-end Smart Metering System? What other options should the Government consider? Please explain your reasoning.**
	Trilliant Response: Trilliant believes that either DCC or a designated third party should be responsible for the cryptographic key management. Without a single point for the cryptographic key management there will likely be interoperability issues between the different parties. Multiple parties managing cryptographic information would require some level of sharing of information, creating an area of additional risk that could face an attack.
62.	**How do you believe the security approach should be applied to opted out non-domestic consumers? Do you see any issues with the approach? Please explain your reasoning.**
	Trilliant Response: Yes, this approach should be applied to the opted out non-domestic consumers. Security should be applied equally across all of the smart meters otherwise this would be a potential pathway to attack the system.

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION 2. Attachment

An Open, Multi-Protocol Communication Solution for the UK Smart Metering Implementation Program White Paper

Following this page, Trilliant has provided the Open, Multi-Protocol Communication Solution for the UK Smart Metering Implementation Program white paper referenced in the response to question 39.

THIS PAGE INTENTIONALLY LEFT BLANK

An Open, Multi-Protocol Communication Solution for the UK Smart Metering Implementation Program

10 September, 2011

Executive Summary

As the standards are set for smart metering in the UK, a wide collection of companies have come together to support an open, Multi-protocol communications standard that will allow the Smart Metering infrastructure to embrace innovation for the lifetime of the system. DLMS/COSEM is clearly one protocol that should be embraced as part of the UK Smart Metering solution, but choosing a fixed, single-protocol solution has significant limitations that will ultimately limit the benefit of the Smart Metering system. The Multi-protocol solution offers significant advantages over the more limiting, single-protocol DLMS/COSEM-only solution currently under consideration, including:

i. **The Multi-protocol solution allows for continued innovation and rich device support.**
The DLMS-only solution locks in today's technology, whereas the Multi-protocol solution leaves room for the simple integration of innovation and new technologies. The DLMS only solution requires significant extensions to the DLMS protocol to support in-home devices and the hub. As new functions are developed by the protocols used by the devices DECC will have to have additional translations designed and the go to the DLMS UA to update the DLMS/COSEM standard to support them. This will rob DECC of the capability to deploy a rich set of device features in a timely manner.

ii. **The Multi-protocol solution supports necessary functions.**
Battery operated devices, prepayment features and other advanced metering functions require more complex communication than can be effectively accommodated by a DLMS-only solution.

iii. **The Multi-protocol solution is less complex, and requires less computing resources.**
If a translation is necessary in the Communications Hub, as would be required in a DLMS-only solution, the Hub must have sufficient memory and computing power to do this translation. With a Multi-protocol solution, the Hub need only send information to the right source – no translation is necessary. This simplifies the overall system because the head end system and devices can both natively communicate without translation. The world of device communications has settled on this approach as most optimal across the board, and in industrial device communications this is by far the favored approach.

iv. **The Multi-protocol solution is lower cost.**
The Multi-protocol solution does not require translation at the Communications Hub, so the Hub capabilities can be locked down while still allowing change in the meters and other in-home devices. The DLMS-only solution will require coordinated updates to the hub software images to embrace new meter or in-home device functionality, and thsoftware type update is difficult to manage administratively, it is organizationally complex to implement. Itincurs significant operational costs, development costs, and carrier airtime costs, and strain it puts on device resources creates a high risk of early device obsolescence.

v. **The Multi-protocol solution is more secure.**
The Multi-protocol solution allows application level messages to pass directly from in-home devices and meters to the head end without translation, so the Communications Hub does not need to decode or decrypt these messages. In the DLMS-only solution, the Communications Hub is required to translate any non-DLMS application level message so it needs the cipher key. This creates significant security vulnerability in the home.

vi. **The Multi-protocol solution is designed for all devices.**
DLSM is designed for electric meters and only the electric meters in the home network will use this protocol. The other devices like gas meters, hubs, in-home displays and home automation devices use application layers such as those defined by ZigBee. The head end systems are full function processing engines that use operating systems that support many applications. There is no reason to restrict the head end system to one device application protocol given that the in-home devices themselves do not share one application.

vii. **The industry is aligned.**
Companies representing energy retailers, meter vendors, communications vendors, and in-home device vendors, have endorsed the Multi-protocol solution. With broad and extensive experience in device networking and device communications, setting the right standards early in the process is critical, and the broad industry backing for the Multi-protocol solution is a strong validation that this is the right approach for both short-term and long-term success of the UK Smart Metering Implementation program.

In summary the Multi-protocol architecture provides a simple, low cost, and secure solution that enables manufactures of a variety of devices to provide interoperable products. To achieve the full benefits for consumers and the broader UK society, the authors strongly encourage the regulators to embrace an open, Multi-protocol Smart Metering Communications solution for the UK Smart Meter Implementation Program.

Introduction

As the Smart Metering deployment in the UK will be a significant investment, and should last well beyond 20 years, it is critical that the system architecture specified be flexible enough to embrace new technologies, protocols, and standards as they evolve. This can be accomplished with no additional upfront cost, but through good design practices.

The evolution of the internet is a good example of this, where the fundamentals of the underlying protocols have remained unchanged for many years, while the application-layer protocols have evolved to enable new applications. The Internet servers like the Smart Energy System head end systems easily support multiple application protocols like those used by in-home devices.

Our vision is to provide a similar architecture for the UK Smart Metering rollout that allows energy retailers and the UK regulators to embrace new technologies, protocols, and standards as they emerge, providing benefits directly to consumers, to the energy retailers, and to society in a timely manner.

This document is specifically written to address the question of whether the wide-area network interface for the DCC should be limited to DLMS/COSEM, or whether it should be expanded to include multiple protocols, including the ZigBee Smart Energy Profile (SEP) 1.x, and potentially expanding to others over time. In our view, choosing a single-protocol solution unnecessarily limits the applications that will ultimately be supported, adds additional ongoing maintenance costs in the long term, and will stifle innovation that could allow the UK to be in front of the rest of the world in energy innovation.

This document is broken down into 5 sections:

- Section 1 describes some details of the Multi-Protocol Solution and highlights differences with a DLMS-only solution.
- Section 2 describes how the prepayment advanced metering functions is inadequately supported through a DLMS-only solution
- Section 3 describes the long-term support costs associated with a DLMS-only solution
- Section 4 describes how security and privacy are compromised with a DLMS-only solution
- Section 5 describes industry support for the Multi-protocol solution
- Section 6 describes the technical issues associated with the DLMS only and the Multi-Protocol solutions

1 Multi-Protocol Solution Technical Description

Overview

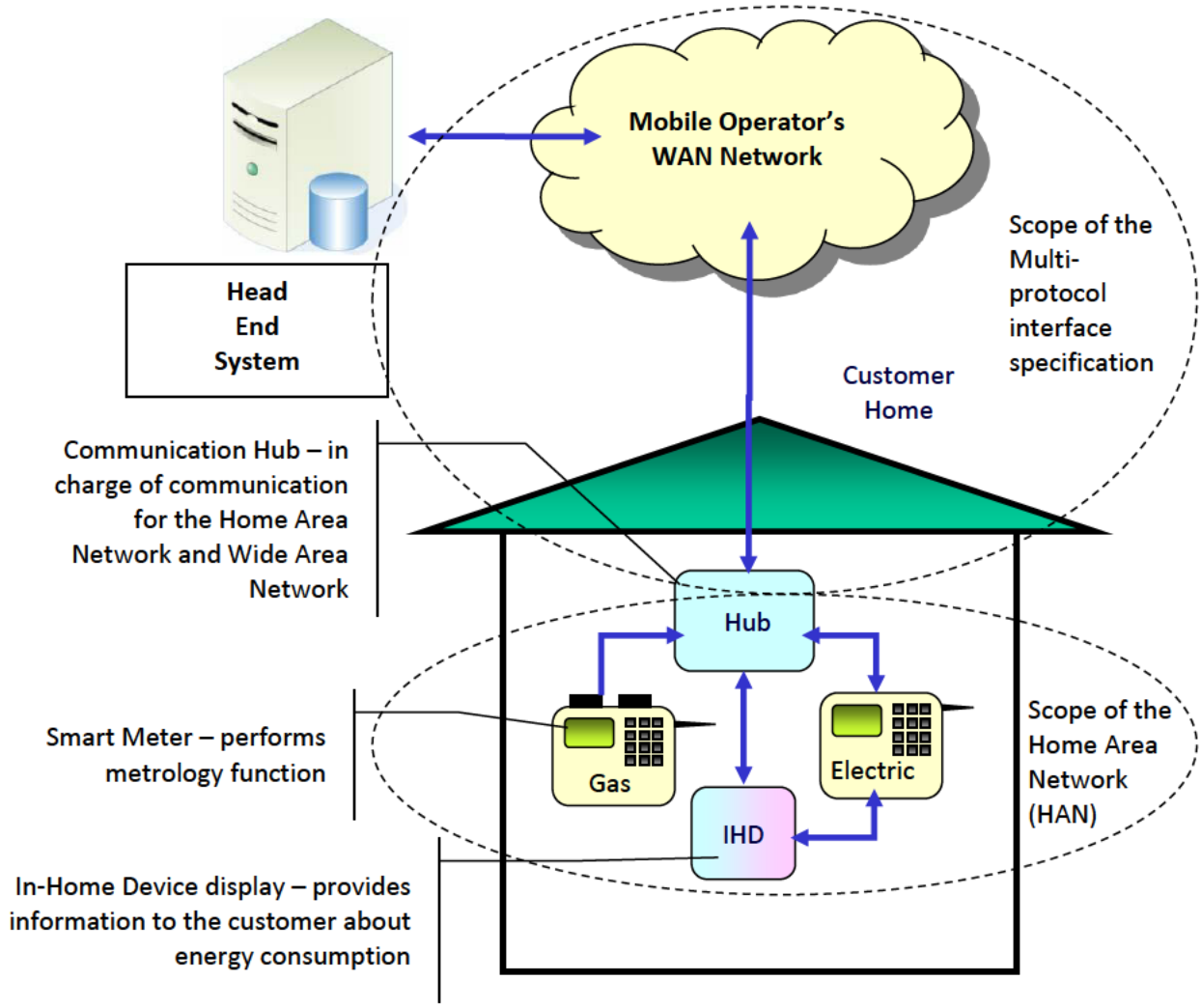
The Multi-protocol solution architecture provides the smart metering system with improved meter data collection and with the ability to send communications to devices in the home. It also provides network management services that make the administration of the system efficient. As illustrated in the figure below, the communications architecture connects two separate networks together to form one system. The WAN connects the remote head end system to the Hub located in a customer's home based on IPv4/v6. The application presentation layer employs the ZigBee Gateway standard, [Ref. 5]. The application layer use DLMS/COSEM, and ZigBee standards. The HAN is a network that establishes connections between in-home devices based on open IEEE802.15.4 radio and MAC, and ZigBee's network stack and Smart Energy Profile Specification version 1.1 R16, [Ref. 1] application layer. The Hub is the gateway between these two networks, and it provides services to the head end system and the HAN devices.

In this reference architecture, the Communications Hub (hub) establishes secure HAN links between:

- The Gas meter and the hub – for communicating gas data and meter management data during scheduled periods when the battery powered Gas meter turns on its radio
- The Electric meter and the Hub – for communicating Electric meter data and for managing the Electric meter
- The in-home display and the hub – For communicating Gas meter data and Unity information to the customer and for managing the in-home display.
- The in-home display and the Electric meter. – For communicating Electric meter information to the customer.

Any of these devices can use either ZigBee SE1.1 or DLSM/COSEM as the application layer. However, typically the Electric meter is DLSM/COSEM and the other devices are ZigBee SEP1.1.

The smart metering network in the figure below shows one Electric meter and Gas meter, but the Hub may support multiple devices. The Hub may also support communication to in-home device appliances.

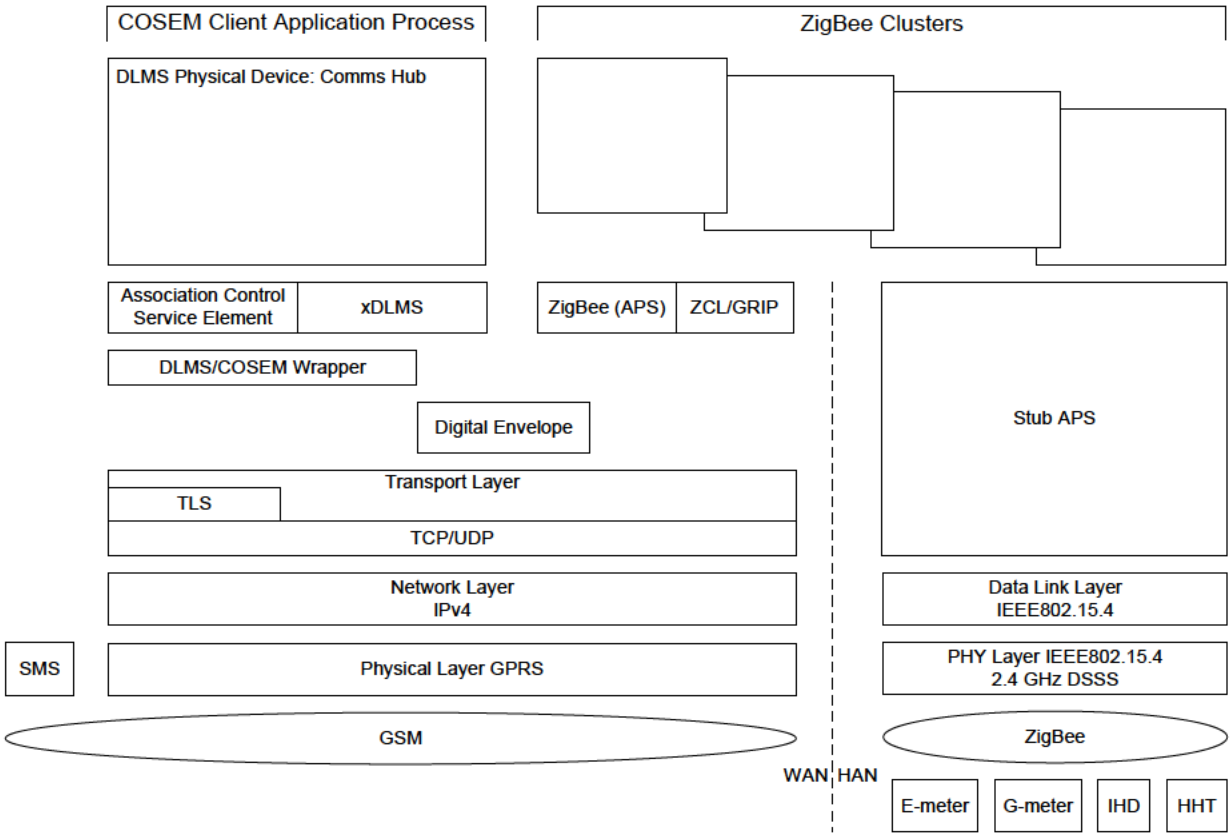


Data Flows

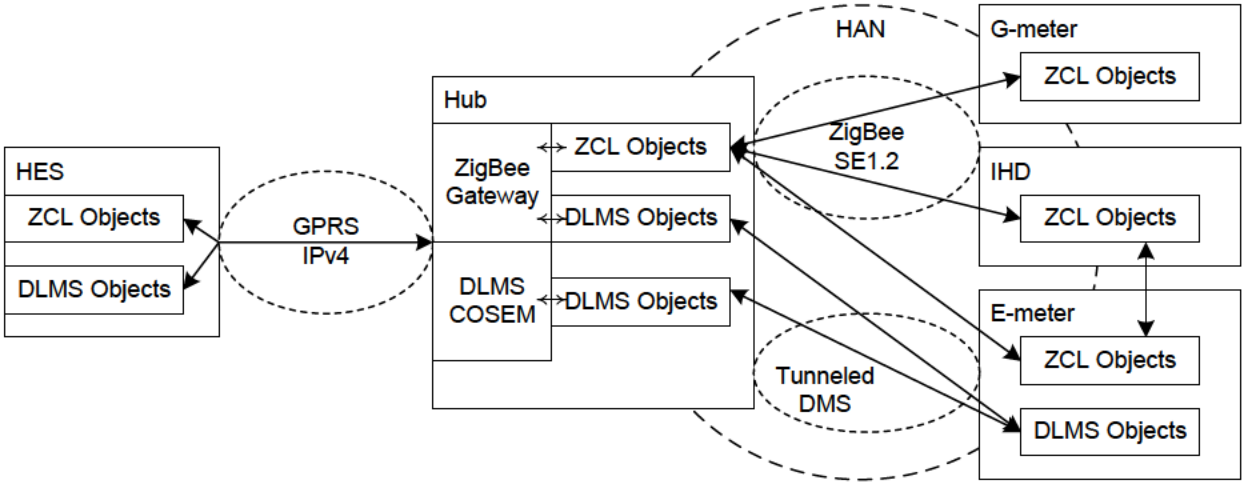
The data transmitted over the connection uses the IPv4/v6 Network Layer and an IETF Transport Layer protocol. The IP transport port numbers are used to direct messages to different devices. The DLMS/COSEM TCP and UDP port 4059 is used for the Hub's DLMS physical device client application process. The ZigBee Gateway Device's (ZG) secure IP port assignment, 17756, is used by the head end system to communicate with the different HAN devices' application layers. The connection to a device's application layer is through the Hub's communication layers.

TCP/TLS is used at the IP transport layer for head end system initiated communications and secure UDP is used for push messages from the Hub.

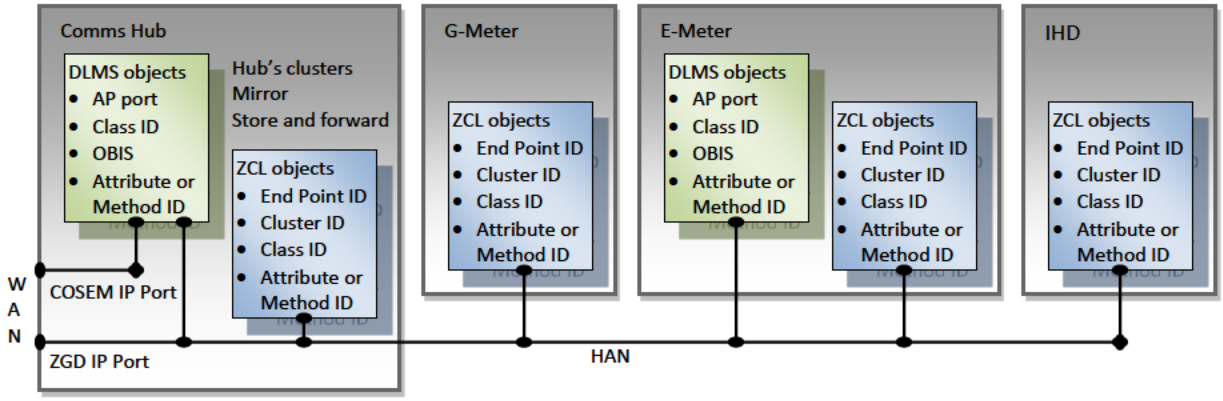
WAN messages use TLS security protocol for TCP and digital envelope security for UDP. The digital envelop layer is above the transport layer and below the DLMS services layer and the ZigBee APS layer.



TCP/TLS DLMS messages use the DLMS/COSEM transport layer wrapper. This wrapper identifies the source and destination client application processes within the device. The DLMS/COSEM application sub-layer Association Control Service Element provides services for the client application processes. These services include setting up the association of the client application processes between devices. The DLMS services include get, set, action, event notification, and trigger event notification. The ZigBee ZCL and Grip layer is used by the ZigBee Gateway described below. The ZigBee Gateway allows the head end system to communicate with the DLMS and ZigBee objects in the HAN devices and Hub.



The COSEM communication profiles for use on IPv4 networks are defined in the DLMS/COSEM Green Book, [Ref. 6] Section 7. They provide the head end system with the ability to communicate with the DLMS objects of the different Application Processes (AP) of an IP addressed node, the Hubs in this case. The DLMS protocol, supported on IP port 4059 of the Hub can't be used natively to access the DLMS objects implemented by HAN nodes such as the Electric meters or the HHT. This protocol also can't be used to access the ZigBee ZCL objects implemented by the Hub or any of the different ZigBee HAN nodes. The ZigBee Gateway specification, [Ref. 5] implements remote interactions with ZigBee devices. The ZigBee Gateway protocol may be used access both DLMS and ZCL objects on the Hub and any of the devices on the ZigBee network.



The head end system communicates with the Hub DLMS objects through the COSEM IP port, 4059. The head end system uses a second port, the ZGD IP port, to communicate with the Hub's ZigBee objects. The ZGD port is also used to communicate with the HAN devices. DLMS messages sent to the HAN devices use the ZigBee DLMS Tunnel cluster to transmit across the HAN. ZigBee ZCL devices used the native ZigBee protocol across the HAN. The ZigBee Gateway defines a set of functions which are organized into the following categories:

- The Application Support Sub-Layer (APS)
- The ZigBee Device Objects (ZDO)
- The ZigBee Cluster Library (ZCL) objects
- The other Communication (COMM) layers, such as the Network and MAC layers
- The Gateway Management Objects (GMO)

The ZigBee Gateway specification used by the head end system implements GRIP Remote Procedure Calls (RPC) and the ZCL function category. The ZigBee Gateway components implemented by the Hub are the GRIP Remote Procedure Calls and the ZigBee Cluster Library (ZCL) functions. The ZCL interface of the ZigBee Gateway allows interaction with any:

- ZigBee device including the Hub itself through the use of EUI-64.
- ZigBee End Point supported on each device through the use of the End Point ID.
- Clusters implemented on each End Point through the use of the Cluster ID. This includes the ZigBee DLMS tunneling cluster to access DLMS objects on a remote ZigBee device.
- Classes within these Clusters through the use of the Class ID.
- Attributes or Methods within these Classes through the use of the Attribute or Method ID.

The ZGD port number is fixed and common to all the hubs.

Comparison to DLMS-Only Solution

The Multi-protocol solution outlined above provides native communications to devices inside the home in their own language. This allows for innovation at the device level and at the head-end system level without updating software in devices throughout the end-to-end communications chain. This technical approach is what has enabled IP networks to become ubiquitous – companies did not have to update their routers when new applications like streaming video because available.

In contrast, the DLMS-only solution requires DLMS/COSEM extensions and translations from DLMS at the hub to communicate to devices using other protocols in the home. This translation can be simple if all of the requirements are known at the time of design, but the Smart Metering system deployed in the UK should support evolution over time, and it cannot be known at this time what devices will ultimately be deployed in the home. Home appliances, home entertainment devices, and home energy management systems are all under discussion, while in-home displays are the only devices that are committed and well defined.

This translation required at the Hub for the DLMS-only solution therefore provides a small barrier today, but a long-term barrier to innovation. The open, Multi-protocol solution provides an evolution path that can be compatible with the Hubs that are deployed in the early phases of the project.

2 Prepayment and Advanced Functions

The ZigBee SE1.1 standard has basic functions for prepayment and extensions have been submitted for inclusion in SEP1.2 for which a working group has been formed. These extended functions include support for prepayment on sleepy devices, managing credit, reporting credit, and getting top ups, credit adjustments and emergency credits. The ZigBee extensions also provide end-to-end authentication security for sensitive data. The Multi-protocol solution supports Prepayment and the extensions and preserves the application layer, end-to-end security.

The DLMS only solution is still working on supporting prepayment and has not yet submitted its work to the DLMS UA.

3 Cost Analysis

The initial costs and long term support costs are both important for consideration for the hub protocol.

Initial Costs

The initial costs are driven by the hardware costs and provisioning complexity. The provisioning complexity is nearly the same in the case of a Multi-protocol solution or a DLMS-only solution. The Communications Hub hardware cost for the Multi-protocol solution can be expected to be slightly less for the Multi-protocol solution than a DLMS-only solution, because it will require less firmware translation. This box can be more like a router – it is not required to have application-level knowledge or translation capabilities. The overall cost difference will be small, but the memory and processor savings will make the Multi-protocol Hub less expensive and less likely to be made obsolete by memory and processing limitations.

This last point is very important. Not many communications devices like cell phones have lifetimes past a few years unless they are the system design places complexity in the head end system and not the device. The Multiple Protocol architecture does this for the Hub.

Lifecycle Costs

The lifecycle costs for the two solutions can be dramatically different. Each time a firmware update is sent to a device, there will be the significant costs of:

- **Firmware development.**
  The hub requires a firmware image, and the development and testing of this firmware can be quite expensive, particularly if it is expected to be interoperable with a wide variety of different devices.
- **Carrier airtime.**
  The firmware images are deployed over the carrier GPRS network, and carrier airtime charges will be incurred.
- **Management.**
  Managing the firmware download to millions of devices can be complex and time consuming. Exception management can take significant staff time.
- **Obsolescence.**
  As feature sets increase, older Hubs with limited memory may become obsolete, and these may have to be replaced. The likelihood of obsolescence is determined by the capabilities of the device at the time of initial deployment and the cumulative changes required to the device over time.

An open, Multi-protocol solution provides much lower lifecycle costs because:

1. **Fewer firmware downloads.**
   As new in-home devices are brought to market with new capabilities, the Multi-protocol Hub can support these new devices without any new firmware update. This greatly reduces the number of firmware images that need to be downloaded to the Hub, and greatly limit the growth of new features in the Hub.
2. **Lower obsolescence risk.**
   Because the Hub does not need to be changed to support these new features, the device memory and processing capability is not be exhausted with translation tables and capabilities, so the devices are much more likely to be useful long after deployment.

4 Security Considerations

The Smart Metering System transmits sensitive information through devices that are not physically secure. The devices may have tamper detectors, but that does not ensure that they can't be tampered with. Even the WAN and HAN network that have protections to keep messages from the outside from entering the network can't be relied on for complete security. Therefore it is important to have end-to-end security available for sensitive data. The end-to-end security ensures that data comes from the source and no other device and that it has not been altered.

The ZigBee applications that have been submitted to the SE1.2 working group include end-to-end application level security for sensitive data. An example of this is the extensions to the Prepayment cluster where sensitive data is signed using the private key of the originator and verified using the public key of the receiver. The Multi-protocol solution preserves the application level security and no trust is place in the Comms Hub's ZigBee Gateway function. With this solution the head end system and the end devices can detect data that has been altered or spoofed by any third party device including the hub.

The DLMS/COSEM protocol can't provide end-to-end data security through a translator in the hub and no solution has yet been proposed for the DLMS extensions that are being worked on.

5 Status and Industry Support

The SSWG (Smart Specification Working Group) is working on the fully formed Multi-protocol interface specification, and multiple energy retailers are currently planning to roll out systems based on thel approach. This open, standards-based approach has widespread industry support not only from meter vendors, who form the core constituents of the DLMS protocols, but also from in-home device providers, who are more heavily invested in the ZigBee protocols. There is very little technical risk in this Multi-protocol solution since the open approach is already well established, multiple vendors already support it, and multiple retailers are already committed to it.

6 Technical Issues

DLMS Limitations

- Over-the-air firmware updates:
  The in-home devices will occasionally require coordinated image updates when upgrade image for one device is not compatible with an un-upgraded image on another device. The coordination requires that the images be upgraded in a sequence or simultaneously and with a minimum amount of time during which the devices are incompatible. The DLMS protocol does not handle this case. It only deals with individual image files and does not have the concept of a sequenced activation in the firmware update protocol. The Multi-protocol solution has a firmware update protocol that transfers image sets that can contain multiple images for multiple devices. The image sets allow the operator to specify timed activation or sequence activation. Unlike DLMS, the Multi-protocol firmware update protocol can transfer one image over the WAN to multiple devices on the WAN saving time and network resources.

- Efficient daily meter reports:
  the bulk of the data transmitted on the WAN are the daily meter reports sent from the Hub for each metering device connected to it. DLMS/COSEM does not have an efficient method for doing the fundamental operation. It requires a full session and association be set up and taken down to transmit a bulk data message. The messages it supports that don't require an association only transmit a single attribute at a time. This limitation seriously impacts both the WAN resources and the head end system resources. The Multi-protocol solution uses a Push protocol for daily meter reports. The Push protocol does not require a session setup or an association. It uses a secure and reliable datagram algorithm that significantly reduces the WAN data connection time. It also reduces the head end system resources by an order of magnitude.

- Efficient network time synchronization:
  The Smart Meter System requires daily hub time synchronization with the head end system to maintain an accurate network time for metering functions. The DLMS/COSEM protocol requires a session and an association is setup prior to updating the time. Like the daily meter reports, this has a significant impact on WAN and head end system resources. The Multi-protocol solution uses the daily meter read Push message acknowledgement to transmit a secure and authenticated time update to each hub. This same WAN resources and reduces the work of the head end system.

- The DLMS/COSEM protocol is designed for electric meters.
  It requires extensions to manage and monitor hubs gas meters, in-home displays and other home automation devices. Some of these extensions are being developed by the SSWG DLMS

group and will require adoption by the DLSM UA. The Multi-protocol solution can use the DLMS extensions but does not require them. The Multi-protocol interface specification that has been published does have some new protocols and ZigBee clusters defined, but the extent of the new material is small compared to the DLMS extensions because ZigBee already supports many of the in-home devices.

- Sleepy devices:
  The gas meter is a battery operated device that puts its radio in sleep mode most of the time to save battery energy. The ZigBee protocol used by the Multi-protocol solution supports sleepy devices through the mirror functions. The DLMS/COSEM protocol does not have support for sleepy devices. It has no support for mirrors and generally expects to be able to communicate with a device at any time.

- Multiple device support.
  The ZigBee protocol used by the Multi-protocol solution has explicit support for multiple meters of the same type. Each ZigBee cluster that supports a particular device has a has a ZigBee Cluster ID and Endpoint ID combination that is unique to each device commissioned on the hub. DLSM/COSEM does not explicitly support multiple devices for each IC. They have to be supported by careful usage of the OBIS codes.

WAN Management Message Overhead

Concern has been expressed about the additional overhead required by the Multi-protocol solutions use of the ZigBee Gateway protocol. While there is additional overhead, as shown in the table below, the amount of additional overhead is very small and will be an insignificant data load on the network.

You will find in attachment an example of a DLMS session implemented using the ZigBee Gateway protocol. The following table summary the size of the ZigBee Gateway header and associated DLMS payload and the size of that same payload used in the DLMS only solution for each of the message transferred. The ZigBee overhead represents the additional bytes used to transmit the DLMs payload. The full packet overhead includes the IPv4/v6 header, the TCP header and the TCP overhead

	Management Request		Hub Response	
	ZG overhead	DLMS payload	ZG overhead	DLMS payload
COSEM-OPEN	36 bytes	38 bytes	32 bytes	51 bytes
GET (0-0:96.1.0.255)	36 bytes	22 bytes	32 bytes	31 bytes
GET (0-0:1.0.0.255)	36 bytes	92 bytes	32 bytes	91 bytes
GET (1-0:x.8.x.255)	42 bytes	212 bytes	38 bytes	148 bytes
COSEM-RELEASE	36 bytes	10 bytes	32 bytes	10 bytes

In fact, the Multi-protocol solution reduces the overall overhead by concatenating multiple management messages into one packet. In cases where this is done, the WAN usage is significantly reduced.

The overall impact the Multi-protocol usage of the ZigBee Gateway protocol on the WAN is small because the management data send is small compared to the daily meter reads. In a Smart Energy System management messages are sent as a result of customer interactions, customer service changes, tariff changes, and firmware upgrades. These are relatively rare operations compared to the daily meter reports that are generated for each metering device, so the small additional protocol overhead in these

cases adds only insignificantly to the overall data load. The head end system, management function will typically do small number of operations a year on a hub compared to the 365/meter daily reports. Estimates for the movement operations are about 5% of the daily meter read operations., so the additional ZigBee overhead is not very important to the overall WAN efficiency of the Multi-protocol solution. The important comparison is the efficiency of the daily meter reads with is optimized by the Multi-protocol solution.

Code Support

The issue of code support for equipment developers has been raised.

The standard DLMS implementations have third party code available that assist in the development of both the head end system and the in-home devices. However, the DLMS extensions required for the DLMS only solution do not have third party code support.

The Multi-protocol solution uses several components that have third party code support. There are mainly in the areas of ZigBee stacks that implement the SEP1.1 functions and in the security algorithms used to secure the WAN communications.

Multiple Protocol Management

The DLMS only solution has be promoted based on the argument that supporting only one application protocol on the head end system makes it easier to design and manage. This is simply not true. Network servers like the head end system run many application protocols for the backend business systems and IT network management functions. The in-home device protocols are no more complicated to develop and manage as these other applications. The IT department routinely manages multiple applications on both servers and PCs on a daily basis.

The DLMS solution actually adds a third protocol, translation, to the hub that has a more serious impact then adding ZigBee to the head end system. Given the choice of where added protocols and complexity should be added to the system, the clear answer is the head end system and not the hub.