over 90% of expected smart meter deployments.

b. British Gas and E.on have already stated that their default HAN solution will be Zigbee and British Gas has begun deployment. Further development is being progressed through SSWG and we support the work that is underway to create a version that meets the UK metering requirements. We are unaware of any plans for deployment of any other HAN technology in significant volumes.

c. Pragmatic actions can be quickly taken forward to mitigate other interoperability issues. We would be pleased go through these in more detail, but they include:

  - The first smart meter installer must not use a HAN that cannot support the other meter and the second installer must not use a HAN that is different to the one installed; i.e. only one HAN per premises.
  - An Industry data item is added to record the HAN installed in a premises so impacts of any difference in HAN can be mitigated.

36.7. However, it is essential that DECC provides assurance to suppliers installing smart meters in the Foundation phase that, subject to complying with the criteria it specifies beforehand, assets will not be prematurely exchanged.

36.8. The appropriate solution for 'difficult buildings' (such as tower blocks, or secluded gas meters) is more problematic and may benefit from some facilitation during Foundation. It is important for the industry that the solutions do not proliferate and that trials produce objective conclusions that can be shared between parties. Suppliers may wish to deploy solutions that might not be available as a European Standard, or meet the full IDTS functionality, and British Gas believes (provided commercial interoperability is supported) that this approach should be acceptable.

36.9. We are supportive of further work by DECC to establish the propagation of different potential solutions, though that is just one criterion in the decision-making process. An improvement in the propagation of one solution over another may be far outweighed by other characteristics of the candidate solutions. It is important that the evaluation criteria upon which any decision on HAN can be taken is agreed in advance of any trialling activity and is transparent.

Question 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.

37.1. The Zigbee Alliance is well down the path of recognition of Zigbee as a European Standard and we expect this to have been completed before 31st December 2014. Our view is that it would be irresponsible to rule out Zigbee on the grounds that this process has not yet been formally concluded so we agree with the recommendation and with the suggested timeline. This date is later the than the proposed start of mandated roll-out however so may prove somewhat redundant. The pace is not entirely within the control of energy suppliers, vendors or the UK so to impose an arbitrary and inflexible deadline may be unwise and pose significant difficulties in the event of unavoidable slippage. We would recommend that DECC require that there be a credible plan presented by the technology providers for recognition as a standard by December 2014.

Question 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.

38.1. There is no merit in introducing a regulatory obligation unless the Government is committed to making a decision on the HAN standard that should be adopted. Left to the market, at some risk to suppliers, the ‘winners’ will emerge. If that takes a long time, the industry will carry the additional costs for years as redundant technology is replaced within its operational life. The question then becomes one of whether regulation would expedite the selection of the 'approved' protocols, or slow it down

38.2. It is in suppliers' interests to reduce technology variation so a rapid conclusion to the period of uncertainty would be welcomed. We are not convinced that Government would be prepared to own the risk of an imperfect decision and that it would therefore be late into Foundation before any conclusion would be reached. In practice those suppliers most active in Foundation will be most influential in determining the direction taken. In taking the commercial risk, that is a justifiable outcome and also the approach that is most likely to deliver the best decision.

38.3. British Gas expects the Government to support the industry decision on HAN, if volume deployments provide the anticipated successful outcomes during Foundation. If a suitable technology is selected by Industry, is proven to be an open standard, is a European work item (as part of M/441), can demonstrate mechanisms for interoperability, then this should become the enduring solution post-Foundation if proved successful.

38.4. As described in paragraph 36.8 above, we think there is merit in 'facilitated collaboration' between suppliers in trialling HAN solutions of difficult buildings.

Question 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?

39.1. No, British Gas does not agree with the proposal to have a single defined application layer standard protocol on the WAN and translate to another on the HAN within the communications hub. British Gas believes that a better method is to adopt a dual-protocol approach on the WAN, using the native protocol of the device over the WAN, to remove the need for a translation layer within the communications hub.

39.2. British Gas made this point repeatedly in the application data layer working groups and the Working Group Options Paper recommends:

'DLMS COSEM and Zigbee SEP1.x each offering different benefits dependent on which meter they are interfacing to.

a. DLMS is more suited to electricity metering applications and can be transported over a number of different media for both WAN and HAN
b. Zigbee SE is more suited HAN applications where low power consumption is a priority (gas).
c. The option exists to run either protocol over both WAN and HAN, thereby providing options for the future and allowing flexibility and future innovations whilst the Application Layer remains unchanged
d. Both of the protocols have a high level of security.
e. Both are European standards or on the way to becoming one.
f. They have the ability to support the Smart Metering System requirement with relatively little development'

39.3. Translation will add to the number and complexity of the lines of code deployed onto the communications hub. This code provides no additional functional value to the communications hub but provides an additional risk of hub failure. Exhaustive testing to ensure that all translation paths are exercised will be required for each release of firmware to the communications hub. There will remain an increased risk to the communications hub of obsolescence and physical replacement cost.

39.4. The proposal to use a 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 go to the DLMS User Association to update the DLMS/COSEM standard to support them. This will deny DECC the capability to deploy a rich set of device features in a timely manner. British

Gas believes a dual protocol approach allows for continued innovation and rich device support, with easier integration of new technologies.

39.5. Battery-operated devices, prepayment features and other advanced metering functions require more complex communication than can be effectively accommodated by a DLMS-only solution, whereas a dual protocol solution fully supports the necessary functions.

39.6. With a dual protocol solution, the overall system is simplified because the head end system and devices can both communicate natively without translation. The world of device communications has recognised this approach as the most optimal, and in industrial device communications this is by far the most-favoured approach. This simplification reduces management costs as the communications hub needs only to send information to the right source, with no translation required.

39.7. We believe that DECC should not specify a WAN Application data layer standard for foundation phase meters.

Question 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?

40.1. Yes, we agree that DLMS and Zigbee SEP1.x should be adopted as the application layer for communications within the HAN, but we disagree that this is dependent on the installation of translation equipment within the consumer premises. For the reasons given in our responses to Questions 39, 48 and 49, we believe that greater efficiency of operations and change management is available from locating all translation processing at the head end, within the DCC.

40.2. DLMS is not suitable for domestic gas meters and, while there are data objects in the protocol for gas, these are designed for use in industrial and commercial implementations.

40.3. In addition we can envisage over time the creation of a single HAN application data layer standard. Whilst we do not believe this is possible within the next 12 months (in readiness for Foundation) it should not be completely discounted. Further, in deciding upon the need for and location of translation activity, DECC should consider the extent to which any translation would be an enduring requirement and the implications of redundancy and obsolescence in the design.

40.4. We would have no objection to the deferral of a decision on HAN application data layer such that it was appropriate to align with a delayed decision on HAN transfer mechanism and WAN application data layer protocols.

Question 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.

41.1. We generally agree with the approach described but have a number of observations:

41.2. In paragraph 150 there is reference to the use of common network layer standards and that messages can be sent without the user needing to know anything of the underlying infrastructure. In our experience, the quality of service available from different infrastructures may not be uniform and could still be apparent to the user. This should not be overlooked.

41.3. We do not believe it is essential that each Communications Hub is provided with a static IP address. A major drawback of this approach is that it would increase the cost of the solution. Fixed IP addressing is inherently more expensive than dynamic IP addressing as fixed addressing requires a greater permanent address pool and /or a greater number of permanently-connected Communications Hubs. This imposes higher capacity requirements on the Communications Service Providers which will be reflected in the cost charged for the service.

41.4. We agree that it is better not to mandate a single network layer addressing standard at this stage as this may be unnecessarily restrictive.

Question 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?

42.1. A single network layer address is reasonable as a longer-term objective although this should not be mandated as it is not essential and adds cost. In our view it should also be acceptable to use more than one address scheme for differing WAN technologies as long as unique addresses can be supported and standards are adhered to.

42.2. A further consideration is that the ease with which faulty Communications Hubs are replaced in the field should not be complicated further by the requirement to maintain the same address after the exchange.

Question 43. Do you think that maximum and minimum demand functionality should be included in the SMETS? Please provide supporting evidence for your response

---

43.1. We are unconvinced that there is a proven case for inclusion of this functionality within the meter as we would have expected the existing data or SCADA to inform DNOs where the networks are under stress.

43.2. If the consumer is open to utilities accessing data on the meter, the half-hourly data will be suitable for providing maximum and minimum demand values for each fuel type. The DNOs should be positioned to run whatever analytics are required to inform their network maintenance and reinforcement programme-planning process.

43.3. It is important to support all stakeholders in extraction of data to ensure that data is only taken once and shared amongst appropriate parties to prevent duplication of communications. There is no supporting business case for including the functionality, as a consumer who opts out of data collection will not allow removal of this demand data unless it is connected to a supplier tariff structure.

Question 44. Do you think that network registers should be included in the SMETS? Please provide supporting evidence for your response (including the cost implications for Smart Metering Equipment, and any alternative approaches that would provide this functionality).

44.1. We see no justification for introducing additional registers to, effectively, duplicate the data already recorded within the meter. The recording of consumption at half-hourly intervals should provide more than enough data for network planning and maintenance purposes. If it is to be used for varying DUoS charges, as is suggested, it is preferable for data to come from a single source rather than be complicated thought the use of additional registers.

44.2. Additional registers would add cost and create a new MID and testing requirement for no obvious benefit. There is currently no justification as, if consumers permit access, half-hourly data is available to support network analytics. Given that this is a new hardware requirement, current smart meters will not support this functionality and the requirement could cause a delay of up to two years (BEAMA estimate). It would add cost into the meter for running concurrent registers, and would require re-approval and significant testing due to the change of 'base meter' design. This could also potentially strand all meters fitted during the Foundation stage even though they are capable of capturing equivalent data.

44.3. DECC consulted on functional requirements of smart metering in 2008 and 2009 making final proposals in July 2010 and confirming these in March 2011. We are therefore very disappointed that this aspect of basic functionality has been introduced at this point in the design process. In itself this suggests that the functionality may be an afterthought that is 'nice-to-have' rather than something critical to network businesses and of value to consumers.

Question 45. Do you think that the prepayment meter contactor switch should be utilised to protect consumer premises from "floating neutral" network faults? Please provide evidence on the costs and benefits to support your reasoning.

45.1. We do not think that this is an appropriate use of the contactor switch. Whist recognising that a potential opportunity to increase safety levels should not be discarded lightly, we do not feel that the case for automated disconnection has been made. Our principle concerns are over setting the correct sensitivity levels for what is a comparatively rare occurrence. We also concur with the remarks in the consultation over the potential additional security risk.

45.2. We welcome the technical study that will look into this question more systematically but it is our expectation that on detection of a 'floating neutral' fault, the damage to consumer appliances and property will have occurred before the switch was tripped. There are no containment benefits, and the network would be required to correct the fault on notification on the network side of the metering installation.

45.3. The smart metering system will not be rated to disconnect the supply during this scenario but, once detected by the smart metering system, an alert can be sent back to the DCC/head end for DNO notification.

45.4. We are also naturally concerned over the potential transfer of liability for such faults from network owners to suppliers. Suppliers are responsible and liable for safety of metering equipment. Network owners are responsible up to an including the cut-out fuse. Placing functionality to address network faults within the metering system could result in a transfer of liability towards suppliers. Further, this could create confusion of accountability and responsibility that could over time increase safety risk rather than reduce it.

45.5. DECC consulted on functional requirements of smart metering in 2008 and 2009 making final proposals in July 2010 and confirming these in March 2011. We are therefore very disappointed that this aspect of basic functionality has been introduced at this point in the design process. In itself this suggests that the functionality may be an afterthought that is 'nice-to-have' rather than something critical to network businesses and of value to consumers.

Question 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.

46.1. The consultation provides a balanced assessment of the pros and cons of the options considered. We agree that these are the only options worthy of serious consideration and also with the conclusion that a separate bridging device provides the required functionality without compromising security or risking the integration of technology that become obsolete during the life of the metering system.

46.2. Further work is needed to establish that there is no security risk, though the threat is certainly lowest with the recommended option. The final design needs to be pragmatic to allow devices easily to join, to encourage take-up, but it may be viewed as a logical place to attack the network. Robust security controls will be required.

Question 47. Do you have any views on the options presented to ensure that electrical contractors can work safely and efficiently between the electricity meter and the consumer unit/fuse box? Please provide evidence to support your reasoning.

47.1. Whilst recognising the opportunity that universal meter replacement offers to upgrade all installations, we do not think that the enormous cost that would be involved in option 3 (double-pole isolating switch) could be justified. Isolation of a supply to allow contractors to work safely on a consumer unit/fuse box can be facilitated by the appointed Meter Operator withdrawing the fuse before the work and replacing it on completion of the work. Provision of an alternative means of isolation eliminates the need for Meter Operator attendance and any resulting delays. However, universal provision of such a facility would ultimately result in costs to all customers for a facility rarely used by many of them. It would also significantly extend the duration of the roll-out. British Gas does fit isolators on all new installations and, if the customer's cables to the existing meter are found to be sub-standard, before exchange. In this situation we will fit an isolator and replace the cables between meter and isolator.

47.2. In all other situations the cost would be prohibitive and unjustifiable in our view, though we may consider offering it as a chargeable service if there is a customer demand. It is likely that the work could be completed at a lower cost than would have been applicable for a specific visit.

47.3. We are not aware of any manufacturer developing a double pole switch within the meter and expect the development and manufacturing costs to work against this as an option. The manual operation of the pre-payment 'load switch' ought to provide the lowest cost solution but we are not persuaded that this would be justified for the limited number of occasions on which it will be required. Option 2, adding an additional mechanical switch within the meter, is expected to raise the cost of the device significantly, unjustifiable for universal provision.

47.4. Option 4, permitting competent non-supply industry personnel to withdraw cut-out fuses, would regularize an existing unauthorized practice. However, the hazards of working at service positions (especially older ones) present significant health and safety issues. A formal training and authorization/accreditation process, including requirements for PPE, safety/security sealing etc. would be required.

Question 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

48.1. No, as we commented in our response to Questions 39 and 40 above, British Gas does not agree with the proposal to have a single defined application layer standard protocol on the WAN and translate to another on the HAN within the communications hub. British Gas believes that a better approach is to adopt a dual protocol approach on the WAN, using the native protocol of the device over the WAN, to remove the need for a translation layer within the communications hub.

48.2. Translation requires that all HAN application protocol layer capabilities are built into the WAN protocol. These protocols are administered by different standards bodies and will require careful analysis, review and agreement to design the translation services, introducing a risk of delay to the Programme. This will be an ongoing requirement if additional capabilities are designed and built into the HAN devices in the future

48.3. Translation will add to the number and complexity of the lines of code deployed onto the communications hub. This code provides no additional functional value to the communications hub but provides an additional risk of hub failure. Exhaustive testing to ensure that all translation paths are exercised will be required for each release of firmware to the communications hub. There will remain an increased risk to the communications hub of obsolescence and physical replacement cost.

48.4. The proposal to use a 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 need to have additional translations designed and go to the DLMS User Association 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. British Gas believes a dual protocol approach allows for continued innovation and rich device support, with easier integration of new technologies.

48.5. Battery operated devices, prepayment features and other advanced metering functions require more complex communication than can be effectively accommodated by a DLMS-only solution. A dual protocol solution fully supports the necessary functions.

48.6. With a dual protocol solution, the overall system is simplified because the head end system and devices can both natively communicate without translation. The world of device communications has recognised this approach as the most optimal, and in industrial device communications this is by far the most-favoured approach. This simplification reduces management costs as the communications hub needs only to send information to the right source, with no translation required.

48.7. As noted in answer to Question 39 the need for translation in either the communications hub or “head end” may be obviated over time by the development of a single HAN application data layer standard. This would render the expensive and complicated development of translation in multi-million communications hubs obsolescent.

48.8. We believe that DECC should not specify a WAN Application data layer standard for foundation phase meters.

Question 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?

49.1. British Gas believes that translation is best managed at the DCC. The alternative would require translation to operate in 30m communications hubs rather than in a single head end. To place the overhead in the communications hub would have an incremental impact on the processing power and memory required and hence impact the unit cost of these devices.

49.2. As enhanced capabilities are developed on the devices, software/firmware updates will be required on the head end, the device and, most significantly, the communication hub. This will add to the time and cost of these enhancements as it will be necessary to synchronise updates to all parts of the Smart Metering system, adding to the time, complexity and cost of delivery and testing.

49.3. As the complexity of code increases so does the number of paths the code can take, the number of exception conditions and the number of test cases that are required to properly exercise the code. Failure to identify and test all translation paths will lead to an increased risk of hub failure and hence increased cost of ownership for this device. Placing translation in the head end protects the longevity of the communications hub as the complexity of the code is reduced.

49.4. The analysis we have carried out to date indicates that there is a negligible effect on WAN overheads when a dual protocol is used. That effect equates to an impact on WAN traffic of between 0.2% and 0.4%. The dual protocol approach[1] was chosen by British Gas as it removes unnecessary translation between protocols in the communications hub. Translation in the communications hub leads to:

---

[1] 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. The application layer uses 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, application layer. The Communications Hub is the gateway between these two networks, and it provides services to the head end system and the HAN devices.

a. Additional complexity and development in the communications hub

b. An increased risk of untested code paths and hence decreasing mean times between failures (MTBF).

c. Increased memory requirements to support additional processing

d. Shortened product lifecycle as a consequence of the additional processing activities

e. Extended delivery timescales for the design

49.5. The dual protocol approach (which transports DLMS and ZigBee application layer attributes and commands over the Wide Area Network) joins IP and ZigBee networks; provided the WAN supports IP traffic, there are no known WAN technology limitations.

49.6. There are three main criteria for measuring the efficiency of a protocol on a network:

a. The time spent on the network
b. The number of octets transmitted on a network
c. The number of packets transmitted on a network

49.7. The time spent on the network can be driven by “round trip times” e.g. the transmission of one or more packets in one direction across the network followed by the transmission of one or more packets in the other direction. The pull model requires eight round trips across the WAN network whereas the push model requires one round trip.

49.8. A simple example[2] to demonstrate the efficiency of transporting two protocols using ZigBee Gateway is the number of packets transmitted in a meter report.

---

[2] There are a number of assumptions in this calculation dealing with:

In a 'pull' meter report the number of packets is 25. The number of packets transmitted in a 'push' meter report is 2. Our analysis indicates that there are significant efficiency benefits to be derived from using a push vs a pull model.

49.9. Where a push model is implemented, there is an average of 36 daily management packet octets generated per meter with a DLMS-only packet. If the same packet is carried in a ZigBee Gateway header the number of management octets generated per meter goes up to 42. This results in the percentage of the total of the management traffic going from 2.8% to 3.2%. Where a pull model is implemented the daily management octets generated per meter remains the same however the traffic management percentage is 0.84% for DLMS and 0.96% for Zigbee Gateway.

49.10. This illustrates that the overhead of the management messages that are carried by the ZigBee process does not significantly affect the overall network efficiency. In this calculation the Push process is used. In the case where a Pull process is used, the overall meter report load is much higher and as a consequence the ZigBee Gateway overhead has even less impact on the system.

49.11. We note concerns that WAN protocols may proliferate without the specification of a single WAN protocol. However the coalescence of Industry towards to HAN application layer protocols can mitigate against any such proliferation.

49.12. In practice we do not believe that there will be a proliferation of approaches to communications hubs or protocols during the Foundation phase. There are only two potential designs being contemplated by the market (dual protocol and pure DLMS). Given the comparatively short time to market during the

---

- The ratio of management packets to meter reports is set to 1%. Typical for consumer services. This is the assumption with the largest impact on the calculation. Increasing the ratio to 10% reduces the improvement to 64%
- The typical management operation is assumed to be an alarm register read. Larger operation like firmware downloads will decrease the improvement.
- Various field lengths such as domain names, country names (estimated name sized used)

Foundation phase we do not envisage many if any alternative approaches being developed.

49.13. There is potential for significant development over time of the available HAN standards, and for the WAN selection to provide new insight in to the most optimum design in this area.

49.14. Whilst concerns may be raised as to interoperability we would point to

a. the very low likelihood of design proliferation as described in 49.12
b. The likely arrival of 3rd party interoperability facilitators as a market response to any interoperability concerns in the market prior to DCC
c. The ease with which Ofgem's commercial interoperability proposals could be extended to include foundation phase meters. Thus requiring suppliers to convert protocols via their own head end solutions in to an agreed format

49.15. We believe that DECC should not specify a WAN Application data layer standard for foundation phase meters.

Question 50. Do you agree that the IHD should only be required to display ambient feedback based on energy usage? Please explain your answer.

50.1. From our extensive deployment, customer research and focus groups, it is clear that the simple Red/Amber/Green indicators on the most widely installed IHD have proved enormously successful and popular with customers. It does not particularly matter, in our view, whether the thresholds are set using monetary or energy units though we accept that if monetary, it would be necessary to recalibrate over time to account for energy price rises.

50.2. The principle requirement is to be able to make the ambient display relevant to the lifestyle/occupancy and property size. If always green or too frequently red the impact is diminished.

50.3. There is clear evidence that the ambient display is the most influential feature of the IHD, but its inclusion within the mandated specification would require the IA to be reassessed, since it is our understanding that it cannot be provided within the targeted cost.

Question 51. Do you agree that Smart Metering Equipment should be designed to support the calculation and/or display of account balances as described above, even though suppliers may not initially be mandated to invoke such functionality for credit customers?

51.1. We agree that there is merit in including this functionality within the SMETS and welcome the flexibility proposed over how the preferred outcome could be delivered.

51.2. There are some complexities in replicating the processing of a major billing system in a distributed network of meters and, even for pre-payment, we believe that the master record should be the supplier billing system. The billing systems account for VAT, dual fuel (and other) discounts, payments, change of supplier, tariffs, calorific values for gas, standing charges, billing periods, etc. It is our expectation that data held on the billing systems will align closely with that on the meters/IHD but it may not be an exact match at all times.

51.3. To date we have found that customers with smart meters welcome the ability to track their energy usage and expenditure and we have had few queries or comments over bills failing exactly to match the numbers on the smart meter. We recognise that expectations could rise in this area however and, therefore, agree that including the facility to display an account balance is sensible.

Question 52. What do you think the costs and benefits are of mandating suppliers to display an account balance (over-and-above those arising from display of information on cumulative cost of consumption) for credit customers on their IHD?

52.1. We do not believe that this is necessarily an issue for the IDTS. The principal impacts are upon the increased frequency with which suppliers must process and reconcile payments with consumption information in their billing systems. Presently this only needs to be done periodically in line with either a monthly or more likely, quarterly billing cycle.

52.2. A requirement for a more up to date account balance on the in-home display will require suppliers to ensure that all the payments they have been received are reconciled with consumption information with the same frequency at which the IHD is updated. Failure to do this will result in significant consumer confusion arising from a misalignment between information on the IHD, information on bills, and the customers own records of payment.

52.3. The costs associated with increasing the frequency of billing system and payment batch runs will run in to £multi-millions as could the costs associated with increased customer contact.

52.4. It must be noted that in the case of PAYG customers, data flows from the prepayment infrastructure directly to the meter so that alignment between customer payment and meter / display is automatic. Whereas for other customers, payment flows direct to Energy Suppliers and realignment / reconciliation activity is required subsequently. This fundamental point appears not to have been understood by many advocates of more frequent account balance updates on the IHD.

52.5. We do not believe that any detailed decision is required on the frequency with which the IHD is to be updated in order to inform the SMETS. Any regulatory policy with regard to do this can be delivered separately and effected by way of supply licence obligations.

52.6. Given that it is probable that the mechanism will exist, we believe that provision of the account balance should be left to the competitive market. If one supplier finds that it is a service differentiator with strong customer appeal, others can be expected to implement it too.

Question 53. Do you agree with or have any comments on the Government's proposals for the outstanding issues from the Response? Please explain your reasoning.

53.1. We support the conclusion of the working group that half hourly update of gas consumption information is a pragmatic approach that avoids undue strain on meter battery life.

53.2. We agree that the requirement to display cumulative consumption within a billing period is excessive and complex to deliver. If the demand exists, this may be more effectively provided through on-line enquiries.

53.3. We agree that there is not a strong case for mandating the display of 'next tariff' rate and the rationale described in the consultation.

53.4. The provision of an enduring pre-payment interface will be site-specific so we support the approach proposed which leaves suppliers and their agents with the flexibility to do what is best for individual customers. It will be rare for the optimal outcome to be a relocation of the meter – disruptive for customers, costly for suppliers and usually reliant on co-ordination with network companies – and we envisage that enhanced IHDs with additional capability for pre-payment (restoration of supply and infrequent entry of transaction numbers) will become common. The industry will be responsible for finding technical solutions to difficult installations.

53.5. The smart meter Data Item Catalogue does not relate to any protocols and it is unclear what benefit it can provide to the protocols selected by the Application Data Group (DLMS/Zigbee). The catalogue has not been used by any industry groups (e.g. SSWG) in development of protocol extensions, etc. If DECC uses this catalogue in its current state to mandate protocol compliance to the data items described, significant delay will be introduced to delivery of full functionality.

Question 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.

54.1. We are supportive of an assurance Framework but this needs to evolve during the programme. What is fit-for-purpose in 2011 will be inappropriate in 2014, and probably undeliverable until 2014 when all stakeholders are in place

54.2. The parties that are most active in the market – some suppliers, most manufacturers, some service providers – are the parties with most at stake and, therefore, with the strongest incentive to protect their investment through rigorous testing. If equipment does not work or is not interoperable then replacement and stranding costs are borne by those who procure and install it – they have most to gain from ensuring it works.

54.3. We advocate a voluntary bi-lateral approach where individual suppliers can work together to validate interoperability or relevant elements of their implementations. For example, supplier one and supplier two can prove that they are able to communicate with each other's metering equipment (similar approaches have been effective in identifying issues and providing assurance in other implementations).

54.4. We do not believe that there is time for an accreditation process to be mobilised in time for Foundation. Even if compliance could be retrospectively applied, uncertainty about the precise compliance regime would undermine confidence and deployment.

54.5. Throughout this period suppliers will be wholly accountable for the security of their smart metering systems (no DCC in place) and existing Data Protection legislation provides strong governance and clarity of obligations in this area.

54.6. In the longer term, there are benefits (for all industry participants) in manufacturers achieving a recognised 'certificate of compliance' which we could envisage being delivered through accredited test houses. We do not think it is necessary for this to be a regulated obligation; in our view once the accreditation scheme is established it will become a minimum requirement for purchasers of metering equipment, much as has happened with CoP5 and CoP10 compliance.

54.7. We envisage a more directly-managed process for the testing of DCC processes and systems interfaces. These cannot be tested by suppliers alone and we see merit in a controlled start-up and 'market-entry' regime. Again, there are parallels with assurance programmes already well-established in the industry, all designed to work for the benefit of existing and new industry participants. In the case of the DCC, any failed processes could also directly impact customers so we would support a strong programme assurance activity under the governance of the SEC. This will also need to provide assurance on the security of connections and connecting parties. The infrastructure could be only as good as its weakest link. We need to get all connecting parties up to the same level of security to ensure the CNI is appropriately protected.

Question 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

---

55.1. The primary objective of testing is to verify that what was specified will actually deliver the technical functionality and required performance. In the context of smart metering the requirements also include interoperability testing, i.e. processes for provision / exclusion of access to specified (but changeable) parties, and the ability to replace components within a system without detrimental impact on the system overall. Functional and performance testing can be separated from interoperability testing and can be delivered through different approaches.

55.2. Functional testing uses the specifications of the component under test as the basis for creating test cases and can sensibly be entrusted to the manufacturers and purchasers of the equipment, since these are the parties with the most 'skin in the game' and, therefore, those with the greatest incentive to minimise their risk.

55.3. For DCC implementation, it is likely that an industry-wide assurance regime and entry qualification process will be required to ensure that failings by one party cannot interfere with the efficient operation of the market.

55.4. Given that suppliers have different appetites and levels of preparedness for Foundation, it is appropriate for testing to be undertaken bilaterally between active participants. Again, the principle of being a stakeholder applies: those suppliers opting to deploy smart meters later should not dictate the test regime for an activity in which they have little or no stake. In contrast, those parties committing earlier to the roll-out of smart metering will want to leverage their investment by ensuring that all customers with suitable smart metering equipment can be transferred seamlessly without detriment to customer service standards and smart metering benefits. Such an approach provides assurance by making those most in need of it accountable for its delivery.

55.5. As the volume of smart meters increases suppliers will be increasingly incentivised to develop, test and implement processes that support change of supplier. This is because the stranding exposure (and risk premiums) associated with potential for premature replacements after a customer loss increases in line with the volume of meters deployed. We anticipate that this collaboration will be led by those most active in the market but will be open to anyone.

55.6. We expect security assurance and testing to be informed by STEG and from experience but do not envisage a security compliance regime to be established ahead of DCC roll-out. It is our view that energy suppliers are more accountable for security than DECC during the Foundation phase because the end to end infrastructure is wholly sourced by energy suppliers

---

Question 56. What are your views on the options outlined for a testing regime? Are there other options that should be considered?

56.1. The strength of the commercial incentives described under the 'market-led approach' should not be under-estimated. The drivers for suppliers and investors to ensure that their smart metering technology and processes are compliant, interoperable and secure, are extremely powerful. In our view, a market-led approach is the right one for Foundation and we would not rule it out for a role in the longer term.

56.2. We envisage stakeholders' interests being protected through testing well in advance of an agreed assurance framework:

a. Asset financier testing

Each 'new' device will be tested by the asset financier, including product tear down testing, analysing what components are in each device, the method and type of manufacturing employed, and also sourcing of the components. This, in conjunction with life prediction testing, will enable asset financiers to provide commercial offerings to purchasers of equipment. This type of testing will be conducted by the MAP, or their appointed test house.

b. Functional testing

IDTS/SMETS: Functional testing will be delivered by setting up test scenarios to prove the functional requirements set out in the SMETS. This can be performed by assessing devices in isolation, or as networked devices. Use cases and processes can be tested using networked devices to ensure the correct outcomes and behaviour are provided by the system/device. This type of testing can be conducted by the Supplier or their appointed test house.

c. Physical/Safety/Bench testing

Independent testing (via a test house) can be performed on devices and systems to prove that physical, mechanical, and safety aspects have been met. Physical testing (for example) will involve proving requirements such as temperature range that might test functionality of non-metrological parts at the rated temperature extremes. Safety testing will be conducted on devices to ensure no harm to the public, consumer, or meter installer and shall include physical design (e.g. no exposed circuit boards), flammability testing (e.g. case materials) and intrinsic testing for gas. Additional bench testing can be conducted to calculate other requirements (e.g. connectivity, life expectancy, system energy use). This type of testing should be carried out by an independent test house.

d. Paper testing

Paper testing will check for all certification (e.g. MID certification), and accreditation (e.g. SMHAN/Zigbee accreditation), declarations (e.g. CE marking and declaration), and overall design documentation (e.g. manufacturer specifications) to ensure conformity to the SMETS and suppliers own specifications. This type of testing should be carried out by an independent test house.

e. Interoperability testing (interchangeability of components)

Technical Interoperability testing should prove that devices using the same SMHAN can be interchangeable between manufacturers. This should test functional checks between devices from different vendors. At present the collaboration that will provide this type of service will be SSWG and their members.

f. End-to-end testing

Once a system has been delivered, ‘end-to-end’ testing will be required to test that the smart metering system works for all functionality (e.g. read to bill, firmware upgrades, mode change etc). This testing may be conducted during integration, so a system integrator or supplier will carry out this type of testing.

g. <u>Change of Supplier testing</u>

Commercial interoperability will be proven between suppliers during Foundation, and this will be achieved by 'change of supplier' and transfer of data via industry flows for meters/devices transferring responsibility between suppliers and their agents. This type of testing will be done by suppliers participating in Foundation on a bilateral basis initially.

h. <u>Security</u>

Security testing will be carried out at both a device and a system level. This testing should be independent and evaluate the products against both the STEG requirements and also the threat analysis work. Security testing should include penetration tests on devices, networks, and interfaces. Testing will need to look at organisation aspects such as segregation of duties, user access management, service continuity, and security interfaces. This testing should be carried out by an independent organisation.

56.3. All the above can be delivered under a market-led approach and does not require an assurance framework. We believe that the delivery of a test specification (see response to Question24) should facilitate a competitive market in the testing of smart metering equipment through accredited test houses. This should enable a 'kite mark' scheme for smart metering equipment that will simplify procurement, bring economies of scale in testing and drive interoperability though standardisation. We have concerns that a mandatory industry code and body could take longer to establish and impose a capacity constraint as new products and firmware releases are brought to market. It is also less likely to be the most cost effective approach, since clients would not benefit from competition in service provision.

Question 57. Do you think that a different approach to assurance is necessary for the Foundation and enduring phases? Please explain your answer.

57.1. In Foundation, suppliers will have more responsibility and accountability for the end-to-end supply chain, the volume of meters deployed will be smaller and there will be no immediate requirement to interface with a new industry service provider (the DCC). Whereas, the enduring solution will have dispersed accountability and a higher volume of meters. The enduring solution will be a part of critical national infrastructure whereas Foundation deployments are unlikely to be, at least during the Foundation period.

57.2. Given that the scope and governance of an assurance regime will take a considerable time to agree, and that (as described in our response to Question 56) it is clear that market-led testing and assurance will deliver similar outcomes (often through the same agencies), the potential cost of an assurance regime in Foundation may be higher since it could create barriers to timely Foundation deployment.

57.3. Therefore, because the costs and benefits of assurance regimes will be different for Foundation and enduring so should the assurance regimes. Whilst we are satisfied that market-led testing is fit-for-purpose and appropriate in Foundation, we would welcome the evolution of an accredited testing regime in advance of the mandated roll-out.

57.4. For DCC processes, and as part of the adoption of Foundation-stage metering systems, we would expect there to be an assurance framework with DCC 'entry testing', a pre-requisite to adoption by and transfer to the DCC.

57.5. We believe that accreditation is simply one method of providing assurance, others exist, such as self-certification. The appropriate assurance mechanism should be determined based on the level of risk to be mitigated. In addition, care needs to be taken that assurance regimes do not distort natural commercial incentives. For example, manufacturers may point to an accreditation as a defence against a liability claim.

57.6. We would note that of the major industry supply chain failures that we have been aware, none would have been identified or mitigated by an accreditation regime. However, market incentives were instrumental in driving remedial action plans.

57.7. We envisage a more directly-managed process for the testing of DCC processes and systems interfaces. These cannot be tested by suppliers alone and we see merit in a controlled start-up and 'market-entry' regime. There are parallels with assurance programmes already well-established in the industry, all designed to work for the benefit of existing and new industry participants. In the case of the DCC, any failed processes could also directly impact customers so a strong programme assurance activity under the governance of the SEC is required. This will also need to provide assurance on the security of connections and connecting parties. The infrastructure could be only as good as its weakest link. We need to get all connecting parties up to the same level of security to ensure the Critical National Infrastructure is appropriately protected.

Question 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?

58.1. This is difficult to answer until we know the detail of the interfaces that must have interoperability. It may be better to allow the existing standards to be used, e.g. TLS allows cipher suites to be negotiated according to capability. Other standards allow a small degree of negotiation (e.g. DLMS) and yet others mandate only one crypto-mechanism to be used (e.g. ZigBee). To prescribe this is to prescribe the detail of the architecture, whereas a more pragmatic approach would be to specify the rules to which the end-to-end metering system must adhere, e.g. STEG requires all cryptography to be FIPS-approved or equivalent.

58.2. The approach to key management must not prescribe the approach to cryptography. To do so would heavily constrain the business end of the system which are most often based on web-services and IP technologies that typically use both asymmetric and symmetric techniques. Normally, the management is not so much of keys but of certificates. On the metering side, to impose a key management regime, implying symmetric, also implies a very significant operational overhead for key provisioning, distribution, rotation, etc.

58.3. It is our expectation that symmetric systems will be short-lived, giving way to asymmetric or hybrid public key solutions. These would use a federated overall solution with national certificate authorities. This should follow the supra-national certificate authority concepts emerging from Europe (Europa smart grid, Expert Group 2) for exactly this purpose.

58.4. It is possible, within this federated model, for the Government to define concepts, standards and hierarchies that allow independently-established solutions to interoperate. We should take care to avoid premature and excessive levels of prescription, since to do so would risk slowing progress towards Foundation. It takes time for industry to react. However, in the longer term, the security approach deployed for the enduring model may need to be more fully prescribed. A key element will be to have a viable migration path from Foundation to enduring solutions.

Question 59. Do you agree that cryptographic/ key management is necessary to secure the End-to-end Smart Metering System? Please explain your reasoning

59.1. Yes, confidentiality and Integrity of smart meter systems and data are necessary to ensure a secure system and to meet DPA regulatory requirements. Without these controls, unauthorised parties could easily gain access to and compromise the system, even if the networks are private. Encryption today is a basic component of any secure solution and we need only look at finance and telecommunications industries who implement this for their business-to-customer interfaces.

Question 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

60.1. We agree with the general comments presented in Table 7 but believe the argument is not sufficiently well-developed to show the advantages of asymmetric techniques over symmetric. We observe that a typical PKI solution is already a hybrid taking the strongest points of the two "competing" cryptographic techniques. We have a revised view of the advantages and disadvantages set out in the table:

Table 7: Advantages and disadvantages of cryptographic solutions

Option	**Advantages**	**Disadvantages**
Asymmetric (PKI)	– No secret information is passed over non-secure networks ~~shared keys used, therefore no need to transmit secrets over unsecure networks~~ - Asymmetric ciphers are stronger than symmetric ciphers. - In PKI asymmetric keys ciphers are nor used for actual message encryption – instead they are used only within a symmetric key agreement process that is applied once at the start of a communication. - Faster, lighter weight symmetric ciphers are used for message protection only once authenticated peers are established using stringer asymmetric techniques - Digital certificates enable clear management rules with well-established principles - Digital certificates can be used to bind the public key to a device (for example, smart meter) or component (for example, DCC systems). This can provide authentication of commands and data, can provide authorisation concepts, and protects against repudiation of commands.	- Specific cryptographic functionality is ~~would be~~ required to be built into the Head-end and Smart Metering Equipment to perform asymmetric operations – this ~~could~~ may slightly increase design and manufacturing costs. - ~~Significantly more processing power required for executing asymmetric key operations on every transaction requiring protection – this could affect system performance.~~ - Asymmetric cryptography is more computationally demanding than typical symmetric cryptography which may impact processor choice for devices such as meters, and may introduce a small communications start up delay. However, silicon providers are moving towards effective cryptographic co-processors within the chip-sets available to meter manufacturers which would eliminate this small concern. As an industry comparison, "Chip and PIN" bank cards already incorporate asymmetric and symmetric co-processors within the chip which is produced at very low cost (and uses very advanced cryptography). - A Certification Authority (CA) hierarchy would need to be established to securely support issuance and management of digital certificates – this could increase running costs. However, this may prove to be very small compared to the operational cost of symmetric key management regimes. The cost of ownership will be related to the rate of certificate "purchase" (signing cost). This could be as few as 1 per installed device but may need a periodic replacement schedule – perhaps every 3-5 years. **The counter-balancing benefit is that certificates can be remotely securely replaced following compromise whereas with symmetric techniques the only secure credential replacement (following compromise)**

		would involve a site visit.
Symmetric	- Less processing power required for symmetric operations ~~– potential to reduce costs and enhance performance.~~ - Symmetric ciphers tend to be faster and do not require heavier key agreement protocols	- Considerable complexity involved in sharing secret keys over unsecure networks. - Symmetric ciphers are less strong than asymmetric ciphers. - Transmission of new keys over a non-secure network typically depends on a single shared secret (also symmetric) (to encrypt the new shared secret) either of which, if compromised, cannot be repaired remotely - Key management is implicitly as weak as the single stored "master secret" as symmetric key agreement depends on a pre-shared secret - Key management tends to need frequent proactive key rotation to reduce compromise risks.
Hybrid	- PKI is a Hybrid system – please see all the discussion above for Asymmetric. (i.e. Asymmetric techniques are used for key exchange and agreement, symmetric is used for message cipher). – ~~•No shared keys need to be transmitted over unsecured networks as these can be encrypted using asymmetric keys.~~ – ~~Digital certificates can be used to bind the public key to a device (or component . This can protect against repudiation of commands.~~	– See PKI/Asymmetric above. – ~~Specific functionality would be required to be built into the Smart Metering Equipment to perform asymmetric operations – this could increase design and manufacturing costs.~~ – ~~A Certification Authority (CA) hierarchy would need to be established to securely support issuance and management of digital certificates – this could increase running costs.~~

60.2. We believe PKI has a number of advantages in terms of the clarity of intent as manifested in various established PKI systems and related specifications. The existence of commercial service providers is testimony to this acceptance in the security industry.

60.3. The primary disadvantage of PKI is the single point of failure at the root certificate authority but this should be treated under normal Information Assurance principles. A secondary disadvantage of PKI is the asymmetric cryptography processing overhead for communications establishment but we believe this is outweighed by the long-term security and operational maintenance advantages (fewer credential updates and the ability to remotely provision updates securely).

60.4. Symmetric solutions appear attractive for their speed and simplicity. However, the key management processes are largely non-standard and always subject to compromised distribution channel risks. The chance of needing to locally update core credentials is greatly increased. Symmetric ciphers are predicted to be "cracked" much sooner than asymmetric ciphers.

60.5. We believe cryptographic co-processor support within cost effective silicon for use by meter manufacturers is the tipping point for this debate. Operationally, and in terms of security, PKI appears far better.

Question 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.

61.1. Yes, it makes sense to have a central hub to assure connections between the meter and suppliers and is critical to facilitating secure Change of Suppler processes. This is also needed to create a 'root of trust' for the PKI infrastructure and, again, it is preferable for DCC to be the 'root of trust' for UK Smart Meters.

61.2. Other options could be to totally outsource PKI to a third party or have suppliers build / run their own and create interoperability processes (as is being done for Foundation now).

Question 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.

62.1. No – any smart system, supplier or vendor which has connectivity to IP networks as part of the UK CNI needs to be appropriately secured. We are starting work now in British Gas Business to understand the material risks and relevant controls to be implemented.