Dear Sir/ Madam

Please find Silver Spring Networks' response to the consultation on draft licence conditions and technical specifications for the roll-out of gas and electricity smart metering equipment.

Silver Spring Networks provides communications modules, software, and networking expertise to the utility industry. We've deployed more than 10 million highly reliable, responsive electric meters across the Americas and Australia. We think that our practical experience and proven scale is relevant, particularly when networking actual utility devices. Our focus in this response is primarily aimed at the technical and architectural questions that have been posed.

We recognize that a number of the areas covered in this response will need further dialog and, as Silver Spring has, in effect, been barred from participating in the programme, would welcome the opportunity to discuss them with the team in more detail.

Question 1: The Government is seeking new evidence and views on the impacts of specifying a completion date that is in the earlier part of 2019.

Silver Spring believes that the 2019 completion date is ambitious but is certainly achievable, and would encourage the Government to continue to strive towards this date.

Question 2: Do you think the licence conditions (AA1-2) as drafted effectively underpin the policy intention to complete roll-out of Smart Metering Equipment by a specified date? Are there any areas where you consider further clarification is necessary? Please explain your reasoning.

No comment

Question 3: Do you agree that the licence conditions as drafted effectively underpin the policy intention to deliver Smart Metering Equipment with the functionality and interoperability required to meet the business case? Please explain your reasoning.

No comment

Question 4: Do you agree that Smart Metering Equipment should be compliant with the SMETS extant at the time of installation and that it should continue to be compliant with that version of the SMETS through the operational life of the equipment? Please explain your reasoning.

If the question is “should something that is being deployed be in sync with the current standards?”, the answer is “yes”. The standards may change, but DECC should set the bar somewhere at each entry point.

Question 5: Do you agree that in some exceptional circumstances suppliers should be required to retrofit Smart Metering Equipment that has already been installed? Please explain your reasoning.

No comment.

Question 6: Do you think that the licence conditions (AA3-6) as drafted effectively underpin the policy intention for the new and replacement installation of Smart Metering Equipment? Please explain your reasoning.

No comment

Question 7: What period of notice do you think would be appropriate before the new and replacement obligation comes into effect? Please explain your reasoning.

12 months. i.e., the notice period for full roll out.

Question 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.

No comment

Question 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?

No comment

Question 10: What role could a dispute resolution mechanism have a role in ensuring interoperability? What key features should such a mechanism have?

No comment

Question 11: For the smaller non-domestic sector do you agree that where there is a Current Transformer meter then suppliers should be required to install an advanced rather than Smart Metering Equipment? Please explain your reasoning.

No comment

Question 12: Do you think that the licence conditions as drafted effectively underpin the policy intention for Current Transformer meters? Please explain your reasoning.

No comment

Question 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.

Allowing for both options 3a and 3b should ameliorate the “gas meter first” scenario.

Question 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.

No comment.

Question 15: What do you think the implications would be of extending the new and replacement obligations to the licences of other relevant parties in relation to installing Smart Metering Equipment in new developments without the involvement of a supplier? Do you think mechanisms other than licence conditions should be considered to achieve the policy objective? Please explain your reasoning.

No comment.

Question 16: Do you think the roll-out of Smart Metering Equipment has any specific implications for the provision of emergency metering services? Please explain your reasoning.

No comment

Question 17: What period of notice do you think would be appropriate before the obligation to provide an IHD comes into effect? Please explain your reasoning.

We remain unconvinced that a mandatory IHD is a good thing. We think that there should be options such as consumer web portals. GB would be the only jurisdiction in the world to mandate an IHD. While the market structure is unique, there is nothing intrinsic to the market structure that indisputably warrants a lowest common denominator IHD. We would be happy to discuss this view.

Question 18: Would the consumer changing their supplier raise any particular issues with regard to the approach set out for the provision of IHDs? Please explain your reasoning.

See Question 17.

Question 19: Do you think the licence conditions as drafted effectively underpin the policy intentions set out for the provision of IHDs to domestic consumers? Please explain your reasoning.

No comment

Question 20: Do you agree that the Standard Licence Conditions identified above require consequential changes in light of the roll-out licence conditions? Do you agree with the Government's proposed approach? Please explain your reasoning.

No comment

Question 21: Do you think there are any other consequential changes to existing licence conditions needed in order to make the proposed roll-out obligations work as intended? Please explain your reasoning.

No comment

Question 22: Do you think there are any consequential changes to existing legislation needed in order to make the proposed roll-out obligations work correctly? Please explain your reasoning.

No comment

Question 23: Do you think there are any consequential changes to existing codes needed in order to make the proposed roll-out obligations work correctly? Please explain your reasoning.

No comment

Question 24: Do you think that there are other requirements that the Government should adopt in the SMETS? Please explain your reasoning.

The most glaring omission from the IDTS is a forward-looking IP architecture. The programme, rightly, does not wish to unnecessarily shut out network technologies, and would also like an open application architecture to allow offerings from many vendors across the entire system: from HAN to head end, from Smart Meter to Smart Grid device. The long-term future is difficult to predict, but it is clear that by adopting a common, proven network convergence layer – IP, preferably, IPv6 – the network will be able to grow and develop no matter what the developments.

Question 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.

Notwithstanding specific comments made in response to other questions, Silver Spring agrees that the remaining requirements within the IDTS be adopted by the Government in SMETS.

Question 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.

The security requirements are a good start, but in our opinion do not go far enough.

SP.15 – One of the biggest threats to a wireless system is over-the-air attacks. Our assumption is that stack smashing attacks and other attacks on the firmware of the system will continue to be viable for a long time to come. An attacker, with enough time and processing power, could extract each and every customer specific credential, or could modify the set of credentials accepted by customer devices to add a credential specific to the attacker. Each and every device in the system needs protection against credential extraction (e.g. the private and operational keys of the device should not be readable by the firmware of the device – they should be used within a secure perimeter). Each and every device in the system needs protection against unsecure operator credential modification.

SP.23 – With no monthly visit by meter readers, tamper evident coatings and seals provide limited or no value. One mechanism may be to require meter-readable seals and have the meter report any breach of such seal. As written this requirement is a no-op.

SP.30 – This is a critical requirement and an appropriate one. However, this has the side effect of making the communications hub into a very very big target. As the communications hub "owns" the HAN, a successful attack on the communications hub is sufficient to spoof any commands to any element of the WAN. The requirement here and below should mandate the shutdown and erasure of critical security parameters for the communications hub if tampering is detected. We strongly suggest uprated security for tamper – FIPS140-2 level 3 or its equivalent – for communications hubs. – SP.34 in particular is too weak.

SP.43 – This requirement is simply motherhood and useless as a means of enforcing security. This, along with SP.50, are operational requirements and have no bearing on the design of the security system – recommend removal.

SP.58 – Instead, "The HAN shall refuse to permit the join of an uncertified device". This can be implemented in the secure protocol, rather than be treated as a throw-away requirement.

SP.60-66 This appears to be mandating a specific approach to top-up pre-payment. We would note that with the connectivity between the meter and the back-end utility, there is no need for a stand-alone UTRN item that can be cryptographically verified by the meter. Instead, a simple purchase reference number is sufficient for the meter to contact the back office for authorization. The form of UTRN presented in this section is also somewhat vulnerable as it tends to be dependent on one or more master keys used to form the UTRN.

Question 27: Do you agree that the process outlined above is a suitable way forward to develop the SMETS? Please explain your reasoning.

Silver Spring has been willing and active in advising the programme on its experience of deploying over ten millions of meters around the world . The programme is making a fundamental error in shutting out organisations with communications expertise (e.g., Silver Spring and others) Such organiztions have not only experience in state-of-the-art communications technologies, but unrivalled experience in security technologies and practice - a vital component of Smart Metering/Smart Grid.

More detail follows in the questions related to security, but it is disheartening, given the public scrutiny under which the roll out will come under, its ubiquity and exposed nature, that security does not appear to be being 'baked into' the architecture. Treating security as an 'end-to-end' problem is a poor approach and risks catastrophic compromise of the system.

Question 28: Do you think that the SMETS should ultimately be governed as part of the Smart Energy Code? What alternative arrangements could be adopted for the ongoing governance of the SMETS? Please explain your reasoning.

No comment

Question 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.

No comment

Question 30: Do you agree that the Government should include a requirement for a Communications Hub in the SMETS? Please explain your reasoning.

Silver Spring agrees that a communications hub should exist and, as we have argued for some time, that the hub should contain more functionality than the basic functionality documented in the consultation i.e., a thick hub. Tunnelling protocols over two potentially lossy air interfaces will be unreliable and byte inefficient. An intelligent communications hub can store data, provide atomicity/handle retries, reduce chattiness (and, consequently byte- and air-time and costs) as well as provide the basis for the type of intelligence that will be necessary to support Smart Grid applications.

Question 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.

Silver Spring agrees the numbers set out in the consultation document broadly reflect the benefits of electricity outage detection. Outage detection has proven to be an invaluable tool both in detecting failures in a prompt fashion, but also ensuring, for large scale outages, maintenance crews can be sure that service has been restored across the entire area affected. Clearly, the benefits will mainly accrue with the relevant DNO, whose interests should not be neglected by the programme.

Silver Spring is surprised, however, that the principle of outage detection is under debate. This is in common use in deployments around the world and has proven its operational worth again and again. The necessary technology is not complex, and indeed, in Silver Spring's deployments the necessary hardware is delivered as standard. Further, we note that with the accelerated deployment of EV charging, inverters on distribution networks, further constraints on networks could lead to grid instability. Outage detection and outage restoration have never been more important.

The most appropriate place for the detection functionality to be deployed is in the comms hub. Algorithmically straight forward to implement (not requiring calibrated circuitry) this reduces the delay in the message being communicated and relies on only a single component (ie the comms hub) remaining operational whilst the message is sent.

Question 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

Yes. The CSP can provide effective event filtering and correlation. This is a function common to all large scale communications network management and has clear parallels in the utility distribution network.

Question 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.

As described above, restoration confirmation messages are an important component of the operational tool kit keeping utilities' costs low and minimising unnecessary call outs. With the right network architecture, restoration messages should cost nothing in terms of additional hardware CAPEX; with the proper retry schemes, even over-loaded star topology TDMA networks should be able to handle the load.

Question 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.

Silver Spring agrees with the modular approach to the Smart Meter/Comms hub, but disagrees that the programme should mandate separate devices. We would observe that the standalone option could increase cost to serve, and add a potentially lossy network to the communications channel, and so we would encourage both options, and believe that the individual suppliers should determine the most appropriate solution for their operations.

Silver Spring is alarmed to note that the technology refresh in 2024 is anticipated to support the needs of the Smart Grid. Initial Smart Grid applications, such as residential EV charging points or Conservation Voltage Monitoring (CVR) are available TODAY and so the Smart Metering/Smart Grid architecture/infrastructure should be able to support these applications from day one.

Text from previous consultation response*: As commented in previous submissions and discussions, we believe that whilst sufficient consideration has been placed upon Smart Metering, much has been neglected within the wider context of the Energy Sector, and this unique M2M (machine to machine) communicating environment.*

Only recently have discussions considered known Smart Grid implications/applications that the WAN architecture could support. Little to date has been considered for emerging global trends and implementations of Electronic Vehicles and Smart Cities to name but two areas.

As the WAN is ubiquitous and could be used for both communication and M2M control, other global deployments are dual purposing the networks for the implementation of Grid and future Grid applications (such as EV monitoring and LV management) and the realisation of Smart Cities (both energy efficiency and social inclusion through data connectivity).

By ensuring that these global implementations are considered, along with the 'art of the possible' we will be able to implement a strategy and infrastructure that is both accommodating and places the consumer at the forefront of the decision making process. By not fully considering the implications of Smart Metering to not just the Energy Sector, but also the UK, we are severely limiting its' operational lifespan and could be creating future additional cost to deploy, as different infrastructure will be needed to realise these emerging markets and requirements.

Question 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 Hub?

Silver Spring believes that the suppliers would be in the best position to determine the most appropriate option for the comms hub. We think a sound compromise would be to allow for both options 3a and 3b.

Question 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.

Silver Spring believes that the Government will have to define a medium to which to connect the communications hub to mandated HAN devices. If other HAN technologies are to be grafted onto the network, it will be necessary to deploy a HAN hub, bridging between the Government-mandated medium and the other technologies. Silver Spring believes, however, that by defining an IP-based architecture, communications to all HAN devices can be achieved, irrespective of the underlying medium.

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.

Yes, Silver Spring agrees that the success of the programme is dependent on the adoption of widely accepted international standards, but that some standards are likely to be under development on the 2014 cutover date. The programme should also put in place a process for adopting further future European standards to ensure that the Smart Grid does not become frozen in time.

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.

No comment

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?

We believe that DLMS/COSEM provides a useful foundation for meter message and device information exchange. Importantly an open and interoperable networking layer approach (that is based on the end to end deployment of the industry standard network layer of IP) provides the flexibility to support and evolve any higher order application that has specified a communication profile based on TCP/IP. In such an approach steps of indirection that require proprietary translation are obviated.

In a separate submission we will be detailing the open architecture benefits of such an end to end IP networking approach.

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?

Both DLMS/COSEM and SEP 1.x afford a useful foundational protocol deployment opportunity. Importantly an open and interoperable networking layer approach (that is based on the end to end deployment of the industry standard network layer of IP) provides the flexibility to support and evolve any higher order application that has specified a communication profile based on TCP/IP. An example of such an evolution is the emergent SEP 2.0 recommendation. It is worth mentioning that state of the art intelligent end-points support such an upgrade (e.g. SEP 1.x to 2.0) through over the air firmware upgrade, protecting investment and avoiding stranded assets.

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.

There is a wide consensus that Internet Protocol based networks (specifically its most advanced iteration IPv6) will serve as a lingua franca layer for Smart Grid information networks (e.g. range of available standards, proven at scale, large development community, built-in security extensions, auto-configuration extensions, expanded addressing, etc). To that end, it is important to differentiate between a useful device and messaging protocol such as DLMS/COSEM, and the industry de facto network layer protocol that is IP. For example, the DLMS UA has specified a communication profile based on TCP/IP, specifically so as to afford data exchange over an IP network layer.

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?

Per the response to the previous question, there is a wide consensus that Internet Protocol based networks (specifically its most advanced iteration IPv6) is the de facto network layer protocol for Smart Grid information networks. Integral to the IPv6 functionality is the capability of Stateless Auto Configuration. An IPv6 standards based end-node (e.g. RFC 2462) will be capable of using such a feature to configure automatically when connected to a routed IPv6 network using Internet Control Message Protocol version 6 (ICMPv6) router discovery messages. Where there are administrative boundaries (e.g. between WAN and HAN) the capability to auto-configure an IPv6 address per administrative domain should be supported (e.g. WAN and HAN separately addressable).

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

The Smart Metering system should form the basis of the Smart Grid and, to that end, will provide valuable tools to DNOs. Therefore this type of functionality should be included in the SMETS if the DNOs demand it.

Further, tariffs that use demand have proven useful in many jurisdictions. Demand functions in meters have minimal (if any) cost and should not be precluded.

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).

See answer 43

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.

No comment.

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.

No comment

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.

Agree option 4 – installers remove fuses

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.

No we strongly advocate an open and interoperable approach that is based on the end to end deployment of the industry standard network layer of IP. Such an open approach affords data-link independence and obviates steps of indirection such as proprietary translation through a communications hub.

Question 49: Where do you believe that translation is best managed:

a) At the Communications Hub; Or

b) At the DCC?

Please see the response to the previous question

Question 50: Do you have any economic, technical or consumer evidence to assist Government in evaluating the options?

No

Question 51: Do you agree that the IHD should only be required to display ambient feedback based on energy usage? Please explain your answer.

No

Question xxx: 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?

No comment

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?

No comment

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.

No comment

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.

No comment

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

No comment

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

No comment

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

No comment

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?

The activities proposed are incomplete. In particular, the activities listed should be preceded by the development of the requirements for such a system. The requirements development should be followed by a review of existing technology – for example Transport Layer Security, Simple Network Management Protocol v3 Security and the Internet Key Management Protocol used with the IP Security Protocol – to determine if needs can be met in whole or in part from that technology prior to beginning a design effort.

Two particular requirements that seem to be missed at first in most Smart Metering (or in the US, Smart Grid) efforts are the lifetime requirements for any cryptography based on the expected lifetimes of the deployed devices, and the need to replace the theft-of-service deterrent represented by the monthly inspection of the meter by a meter reader. Both need to be considered in the formation of security standards.

Finally, communications security tends to be a specialist function, and not one that can be well represented by the typical utility operators and vendors that currently dominate the system of utilities. If DCC allows the discussion of security requirements to be dominated by traditional meter vendors and utility companies, it risks deploying a system not fit for the designed purposes and which fails to deliver the promises of the smart grid future.

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

It is alarming that the consultation document states, '…cryptographic functionality may be needed.' Silver Spring Networks' believes that the smart metering system should form the basis of the UK smart grid network and so, as such, will form a critical part of the delivery network over the years to come. That the programme still considers, for a system that will be in place for at least fifteen years, this to be an option is a clear reflection of the influence that non-communications manufacturers are having on the design of the solution. To deliver a system that does not have industry-standard security mechanisms at its heart would leave this massive investment barely suited for Smart Metering and completely unsuitable for wider Smart Grid applications.

Even if Smart Metering involved only remote meter reading and had no related control functions (e.g. remote disconnect, pay-as-you-go), there would be a need for security for the communications path between the smart meter and the utility and/or other cognizant organization. That security will involve as a minimum integrity protection of the data and commands, authentication of the meter to the utility for billing purposes, and authentication and authorization of the utility and other organizations to the meter for control and configuration functions. Providing such security in a modern world requires modern cryptography, good key management and a total avoidance of such things as passwords and master keys.

You should expect that a given meter will be deployed for a lifetime that exceeds 15 years or more. In those 15 years, the ownership of the meter (and/or the customer) may change hands repeatedly. That will require changes in the operational keys of the meter and the meter support system at least with every change and generally more often to maintain security over the years. Setting the key once at deployment will not scale and will not be secure.

With respect to cryptography, we recommend selecting a suite of cryptographic primitives that have been publicly validated and have some form of government (both UK and other) cachet. For example, the United State FIPS140-2 standard describes both hardware and software requirements for cryptographic modules such as those that might be incorporated into UK Smart Metering standards. The phrase "FIPS approved" when applied to cryptographic algorithms and modes provides substantial assurance of a rigorous analysis process. Also, the ZigBee Smart Energy 2.0 standards appear to have settled on the Suite B set of cryptographic primitives as their baseline for security functionality

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

Generally, no security designer would consider a pure Asymmetric system for anything but extremely low duty cycle, small numbers of end point use. Given the general architecture of the system (multiple reads per day, millions of nodes) and the inability of a pure Asymmetric system to scale to those levels, it probably isn't appropriate to even mention Asymmetric as an option.

The mention of PKI in the text is limited to the Asymmetric option, but properly noted as also part of the Hybrid option in the table. For clarity, the paragraph text for the Hybrid option should also indicate a dependence on PKI technology.

With respect to the advantages and disadvantages, the table should consider the ability to maintain security over a long lifetime and the ability to scale to millions of nodes. Both Symmetric and Hybrid have benefits with respect to scale – lower processing power for symmetric cryptography means that a given controller can handle many nodes. Hybrid gets that as well and tacks on a mechanism to derive symmetric keys on the fly for operational use. Hybrid also scales in the ability to not need to store the millions of keys prior to meter deployment unlike the pure symmetric system. Symmetric has an offsetting disadvantage to scaling in the need to store and secure those millions of keys from manufacturing through deployment and the operational lifetime of the meter.

For Hybrid security, in general key agreement tends to be preferred over key transport/key encryption. Both should be mentioned as possible.

Two of the options claim development of encryption mechanisms will incur increased "manufacturing costs", but do not note the concomitant reduction to "operational costs". We would also note that manufacturing costs tend to amortize over time, while operational costs tend to increase. Selecting a solution that is slightly more expensive initially, but will tend to moderate operational costs seems to be a responsible approach.

The programme should also consider that most credible communications technologies are now delivered with state-of-the-art cryptographic functionality. The programme as part of the development of the overall security architecture, may want to consider deployment of such functionality in nodes other than the end meters.

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.

It's unclear that DCC need be responsible for the entire lifecycle of key management for Smart Metering. Instead, it may make sense to use DCC as a clearing house for the transfer of credentials needed to control/manage/read any give smart meter as they transition from one utility to another. The control of that function may ultimately vest in the customer in a system where the customer also controls who its utility provider is.

If we assume a hybrid system with a digital certificate based authentication and authorization system enabling sets of derived or encrypted shared secret symmetric keys for operational use, then it should be possible for each ownership or management change to be digitally and securely authorized at every step of the way. For example, a fully realized system could use a digitally signed notice by the customer to authorize the transfer of their service from one utility to another, and that transfer could be enforced by the meter itself.

DCC may find itself in a role where it's responsible only for exception cases – for example where one utility refuses to relinquish control of a customer to another utility against policy or regulation. To put a finer point on it, it's not clear DCC need have any involvement in the day-to-day operation of the Smart Metering system assuming a well designed system.

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.

For non-domestic, opted-out customer it may make sense to eventually transition them to a similar system as domestic customers, if for no other reason than to simplify utility operational concerns. As there appears no pressing need to do so immediately, the only guidance we suggest at this point is a brief review of the requirements when defined, and eventually a review of the selected approach to ensure that a future transition is not precluded.