Chapter 4 – SMETS 2 Development

1. Do you have any comments on the criteria used in the evaluation of the application layer standards?

   Answer: We have no problem with the criteria used for the evaluation of the application layer standards. But this implementation will be with us for quite some time. The interest is in seeing the plan for making controlled updates to the standards and the provision for updating the devices already in the field with incremental improvements over time. The tunneling of other protocols seems ideal as a strategy for evolution. It is the plan for secure and reliable update that is at issue. If these are well planned, then the initial state seems fine.

   A review of the upcoming GB Companion seems useful, also.

   As interoperability is the major goal, and change is inevitable, then a review of the certification process that allows change at a suitable pace seems important, too.

2. Do you agree with the proposal to adopt ZigBee SEP / DLMS as the HAN application layer standards for GB?

   Answer: As described above, if a practical approach to secure change to the system is in place, the initial approach would be just fine. But, attacks will occur and vulnerabilities will be found. The thought that no change to protocol or foundational logic will ever need to be made is just not in the cards. So the difficulty will be in estimating just how much change will be needed before wholesale replacement must be ordered.

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

   Answer: Yes

4. Do you agree with the overall approach proposed in relation to the HAN physical layer? If not, please provide a rationale and evidence for your position.

   Answer: Yes, but the overall approach should be one that errs on the side of simplicity for both the consumer as well as the installer. The simplistic approach would be to allow the deployment using the 2.4 MHz approach wherever it has adequate coverage to sustain quality communications for the estimated 70% coverage, but maintain the **'fit-for-purpose installation' obligation** on suppliers for the next 25% coverage using 868 MHz communications

adapters. This would act to require suppliers to ensure that the solution they install at any property was capable of serving all the smart metering equipment in that property.

Boosters for both the 2.4 GHz and 868 MHz situations are inevitable for the remaining 5% of the locations.

If there is a need to err, one should always err on the side of simplicity relative to the user experience and to the installer experience. The cost differences between the dual band hub and the cost of labor and confusion will show that the equipment cost saving is a local optimization as opposed to the true low cost approach.

5. Do you have any comments on the criteria used in the evaluation of the physical layer of the HAN?

   Answer: No – this seems well researched. Inevitably the number of frequencies used in the home may expand for commercial reasons over time. We should not think of this as a bad thing, but more of a market consideration to be sorted out separately from the basic approach to the initial scenario described here.

6. What are your views on the compatibility of the reserved spectrum 870-876MHz with 868 MHz and the value of considering the use of this band?

   Answer: In time, the SDR flexibilities and costs of being agile in the home environment will create a new set of opportunities that are not part of today's discussions. We should not rule out the eventual use of the 870-876 MHz band.

7. Do you consider that additional measures should be taken to encourage the development of an 868 MHz solution?

   Answer: No. For simplicity of approach – stick to the simplicity of one frequency and use a repeater if necessary for the special coverage areas. Confusion in time during installation will rapidly erase any benefit of the complexity of two (or more) frequencies.

8. Do you agree with the approach to allow the market to determine the balance between 2.4 GHz and 868 MHz? If not, please provide rationale and evidence.

   Answer: The market will lean quickly towards a simple solution that is more error free and less confusing (i.e. costly) to install.

9. What are your views on the three options identified for displaying wireless solutions (i.e. 2.4 GHz as the default; dual-band communications hubs; or market led)?

   Answer: 2.4 as the default – plus a recognition that a relay may be needed in some cases.

10. Do you agree with the proposal for a 'fit for purpose' installation obligation on suppliers?

    Answer: Yes.

11. Do you have any views on the proposed approach to developing a wired HAN solution?

    Answer: Use PLC as the wired solution where a wired HAN solution is needed where wireless solutions will not achieve satisfactory propagation. This should be studied for the small percentage of GB properties (c. 350,000) that are high-rise flats where wireless HAN solutions are unlikely to work without the use of extra equipment and/or shared infrastructure. This should be considered in the discussion below concerning security in that adequate separation needs to occur between different tenants such that personal privacy is maintained.

12. Do you agree with the proposed scope of functional requirements for a communications hub? Are there any other functions that should be included and what would be your rationale for including those functions (including estimated costs and benefits)?

    Answer: We agree, with slight extensions.

    Here are the specific comments regarding the structure of the device:

    - The device is separate from the meter itself and therefore reduces the complexity of the meter and also ensures more longevity against advances in communications technology and reliability. Making this a requirement will lead to additional simplification over time.
    - The overall structure of the communications hub should require separation of the applications functions from the communications functions from the device management functions.
    - The transfer of messages within the **WAN module** also needs to isolate management functions from application functions for reliability purposes.
        - The management functions need to include the following:
            - Device mutual authentication
            - Authorization for management controls and provisioning
            - Auditing for sensitive events
            - Encryption for the management sessions
            - Integrity checking
            - Availability protection for denial of service via protocol whitelisting
            - Non-repudiability for financial transactions involving functions such as prepay operations.
        - The application functions should include the following:
            - Application service authentication
            - Integrity checking

        - Message validation
        - Message error checking
        - Translation and/or formatting of messages for the WAN
    - The WAN module will need to be designed to match the WAN communications technology (i.e. core and infill WAN technologies used in each CSP region). This will anticipate the current migration toward wireless LTE technologies.
- The WAN communications and the HAN communications should be separated by a firewalling function to maintain security separation between the WAN and the HAN.
- The HAN module maintains the communications hub's connection to the HAN, it provides the 'network coordinator' function for HAN operations, and manages the transfer of messages across the HAN.
    - The **Network Coordinator** function is responsible for establishing the HAN. Both wireless and powerline carrier networks are shared media networks. The Coordinator establishes a unique network, defining a network ID, or other mechanism that makes a given collection of nodes distinct from another that may coexist in the same space. These networks are kept distinct by defining separate network participant domain security keys – typically one for the management virtual network, a separate one for the local HAN network, and one each for participating WAN virtual networks. This participant domain key is a credential used to partition the media from other networks, and is not considered a fundamental part of the security posture of the system, but it is highly related as application security is layered over it.
        - 802.15.4 networks should have one and only one Network Coordinator responsible for establishing the network and defining the PAN ID.
        - HomePlug networks should have one, and only one, Network Coordinator, responsible for establishing the network and defining the Link Layer Network Key (Network Membership Key, or participant domain).
        - This is a single device that is associated with both a HomePlug and an IEEE 802.15.4 network and serves as the Coordinator for both networks.
    - The **Network Access Server** function manages the two relationships that a HAN node may have with a HAN:
        - Unassociated
        - Networked

      A node that lacks any association with any network is only able to perform limited communication with the communications hub which is running a Network Access Server. The Network Access Server is responsible for policing the Authentication transaction between an unassociated node attempting access to the network and the Network Authentication Server. It

relays the transactions between the unassociated node and a Network Authentication Server, which is co-located in the communications hub.

Network Access and Authentication is a separate and distinct process from application level Authentication and Authorization. It is possible, if not likely, in Smart Energy Profile Networks for Network Access and Authentication to be controlled by one primary entity (for example the Consumer), and for application level Authentication and Authorization to be controlled by another primary entity (for example a service provider). It is also possible for Network Access and Authentication and application level Authentication and Authorization to be controlled by multiple entities based on program requirements (for example customer and a Service Provider) delegated by the primary entity. Note: Underlying technologies used in the encryption, Authentication, and Authorization processes may be shared, but responsibilities are separate.

- The **Network Authentication Server** is responsible for authenticating a node's identity and determining whether the node is authorized to join the network. The Network Authentication Server controls the acceptance of nodes onto the network.The Network Authentication Server accomplishes this by checking the credentials presented by the unassociated node (through the Network Access Server) and subsequently accepting the node onto the network and moving its relationship to 'Networked', or rejecting the access attempt. The Network Authentication Server is on the communications hub, but it is controlled by the Consumer (e.g. homeowner). It may receive Authentication credentials (on behalf of unassociated nodes) from multiple Network Access Servers operating on different physical network paths to the communications hub.
- The **Application Trust Center** is responsible for Authenticating and Authorizing applications. When a node moves to the Networked state, the applications which run on the Device become able to communicate with counterpart applications running on other Devices on the network. Devices may be Authenticated and then Authorized to enable many functions.

  There are four relationships that an application may have in the HAN network:

  - Unauthorized
  - Subscribed
  - Enrolled
  - Controlled

  The Application Trust Center facilitates applications moving from the unauthorized state to the Subscribed, Enrolled, or Controlled state in which the applications have an Authenticated and Authorized relationship with other applications serving customer-specific data, or with a Service Provider providing remote services across the WAN. There should be no restrictions regarding which devices may host an Application Trust Center (such as the communications hub itself), or precluding using a service provider

authorization service for this function. Multiple Application Trust Centers may exist within the tailored trustworthy space including the nodes in a HAN network. For example, a distribution Utility may provide an Application Trust Center which is contacted to provide access to metering data. A retailer may provide an Application Trust Center to facilitate access to billing data. Finally, a Consumer may maintain their own Application Trust Center to provide access to home automation services.

In short, application level Authorization should be performed through an Application Trust Center. No application access should be provided except as Authorized through an Application Trust Center.

- The **Energy Services Interface (ESI)** provides a virtual link between the HAN and an Energy Services Provider such as a distribution company or retailer. Typically, the ESI is also the Application Trust Center for the Energy Services Provider in question, but this is not a requirement. Most Smart Energy Profile Networks will have at least one ESI; however, it is possible that a stand-alone HAN would be deployed without an ESI. In this case, if an interface to a Service Provider is needed, the ESI may reside in the Service Provider's network, and alternate approaches to route HAN traffic to the ESI could be utilized. It is also possible that there would be multiple ESIs, for example in environments like deregulated markets where multiple parties are part of the energy procurement and management process, or when there are Service Providers for additional commodities such as gas or water.

- **Processing functions** - this component performs a range of message handling, data storage, and processing functions, for example:
    - As an **application partition** – providing a gas meter 'mirror': this will allow the communications hub to perform various functions as a **proxy** for the gas meter thus reducing the amount of power consumed by the battery in the gas meter. This allows the gas meter and the communications hub to be synchronised at **30 minute intervals** rather than having to respond directly to ad hoc requests.
    - As a **management agent**:
        - Issuing **alerts** on detection of a power outage and the restoration of supply.
        - Support for **firmware upgrades** to the communications hub and, possibly, to other HAN devices.
- We agree with the Government proposal that the communications hub should support two classes of HAN device, namely smart metering devices (essentially meters and the IHD) supplied and installed by an energy supplier, and consumer access devices (CADs). CADs will only be able to access a defined set of data items from smart metering devices on a read-only basis. They would not be permitted to update meter configuration parameters or to execute meter functions.

- Also: access to participating devices at the location that would participate in a demand response program, such as electric vehicle chargers or program controlled thermostats.
- The communications hub would require a power source taken from the unmetered mains electricity supply. It is expected that a standard power connector will need to be specified as a requirement for SMETS 2 electricity meters.
- The CHTS would contain detailed requirements for the HAN module and the processing functions of the communications hub, but only high-level requirements for the WAN module. The detailed specifications for the WAN module would be added by CSPs.

13. Do you have views on the specification for an 'intimate' interface between electricity meters and communications hubs?

- **Answer:** The communications hub could be stand-alone or fitted directly to the electricity meter using a standard 'intimate' interface. The 'intimate' interfaces would facilitate the installation and replacement of communications hubs and offer a data link between the electricity meter and the communications hub, in addition to the wireless HAN link, in addition to the WAN link(s).

14. Do you agree with the Government's marginal preference for the CSP-led model for communications hub responsibilities, or do you prefer the supplier-led model? Please provide clear rationale for the advantages and risks associated with your preferred option.

Answer: CSP-led model.

As described, the CSPs would own the communications hubs and would be responsible for their procurement, certification and testing. Devices would be passed to energy suppliers on consignment to install alongside meters and to install replacements in the event of faults.

The merits of the CSP-led model include:

- It places responsibility for all parts of the WAN with one party so the CSP can be held responsible for providing access to the HAN. ***This is very important when it comes to the matter of assigning responsibility for personal privacy matters.***
- CSPs have a better developed capability than energy suppliers to source communications equipment efficiently and economically.
- There will be fewer CSPs than energy suppliers affording potential aggregation economies when buying from original equipment manufacturers.
- By placing responsibility with a third party it avoids dependencies between competing energy suppliers for non-dual fuel premises where, for example, the gas supplier would otherwise employ a communications hub belonging to a different electricity supplier.

The risks of this approach that need to be managed include:

- It places responsibility for delivering an effective HAN with the DCC as deployed by its CSPs. Further, it requires an agreement between the electricity supplier and the CSP for services including both WAN access as well as the supply of qualified communications hubs to be held on consignment by the electricity supplier and installed by the electricity supplier workforce.
- Responsibility for all in-home equipment would not reside with energy suppliers, in line with their responsibility to consumers. However, this transfers the matter of responsibility for personal privacy issues to the CSP.
- This approach adds the risk of one organization (the electricity supplier) installing another's assets (the DCC) and potentially developing complex recharging arrangements between energy suppliers and the DCC during the period of consignment.

It will be necessary under this approach to operate the principle that 'costs lie where they fall' in respect to installation and maintenance, to avoid complex recharging arrangements.

15. Do you agree with the proposal that a CHTS-compliant communications hub should not be mandated for opted out non-domestic sites and that suppliers should be free to use whatever type of communications equipment best supports their processes and WAN service?

    Answer: Yes.

    This being said, the transition for a domestic site that formerly opted out to a new desire to opt in to take advantage of monitoring services or to realize the benefit of potential demand response programs and then subsequently vacillates back and forth between opt out and opt in status presents a logistical nightmare. It would seem that once a site has ever opted in for service, the CHTS-compliant communications hub should be able to be left in place and then remotely enabled or disabled as the site elects to subscribe or unsubscribe for the service.

    From an architecture standpoint, there should be options on a CHTS-compliant communications hub for interconnections that do not circumvent the security of the CSP network and application services, but allow flexibility in choice of the fundamental communications medium.

16. Do you agree that the gaining supplier should bear the costs of installing an appropriate communications hub if they decide to switch between opted in and opted out?

    Answer: Yes

17. Do you agree that the design and implementation of outage reporting functionality should be assigned to CSPs, documented in the communications hub technical specification?

    Answer: Yes

    Outage detection and reporting functionality covers the capability to detect that a power outage has occurred in consumer premises, to log that occurrence (within the electricity meter) and, if the supply is not restored within a specified period (say, at 3 minutes), to send an alert to the DCC via the WAN. DCC would forward alerts to the relevant DNO. When supply is restored another alert would be issued.

    Outage alerts should be triggered by the smart electricity meter, the communications hub or in components of the CSP's network. The communications hub should be able to store sufficient power to send an alert message after the mains supply is lost.

    The proposed CSP-led model for communications hub responsibilities is recommended and the responsibility for outage reporting should fall within the scope of the CSPs' activities. Responsibility for outage reporting should be included in the scope of the CSP procurement: CSPs may elect to implement the functionality in any of the components of their smart meter WAN infrastructure, including, but not limited to, the communications hub. For convenience, the outage reporting functionality should be specified in the CHTS.

18. Do you agree that it would be inappropriate to require meters operated outside DCC to be required to implement outage reporting? Please provide rationale to support your views

    Answer: Yes. The emphasis should be on conversion to the DCC as opposed to ancillary requirements for change to meters outside the DCC.

19. Do you agree that maximum demand registers should be included in SMETS? Please provide evidence to support your position and provide evidence on the cost implications of delivering this functionality via back office systems or via the meter.

    Answer: Yes. However, to be of use, this data needs to be gathered at the back office for analysis purposes.

    Maximum demand recording requires the electricity meter to identify and record the highest demand value in a given period of time. This data has been requested by DNOs to assist with network planning and the operation of their networks. This data will be of particular value as distribution networks come under increasing pressures arising from renewable generation, microgeneration, electric vehicles, and the electrification of heat.

    Under this option additional registers would be provided in the meter to record maximum demand values. Discussion with stakeholders has indicated that DNO requirements could be satisfied through the provision of three registers, two for import and one for export. One of the import registers and the export register would measure the maximum demand/export in any user-configurable period since the register was last reset. The second import register would measure the maximum demand in a user-configurable period within a larger user-

configurable period (e.g. the highest half-hour demand on any day between 16:00-20:00). The registers could be reset independently of other registers.

Further investigation shows there may be merit in users configuring measurements collected every 10 seconds. As this collection period would be brisk, a further option is that an application be resident in the communications hub that would allow data collection in the communications hub and forwarding aggregate messages to the DNO at a pace selected by the DNO subject to the DNOs ability to absorb messages at that rate.

There is merit in synchronizing the time in all meters adopting a time period set nationally by a body such as the Energy Networks Association. This would be a management agent function within the communications hub that could provide precision time via the Precision Time Protocol as commonly used by wireless communications networks to synchronize bit stream cadence.

While we agree with the DNOs that rapid retrieval of maximum demand register data would be costly if controlled solely by the back office, the use of the communications gateway as a data collection device that forwards the readings at a rate that would make them usable by a demand response system would probably be very useful for load control applications.

20. Do you agree with the proposal not to include the capability to generate additional voltage alerts based on counter thresholds in SMETS 2? Do you have any evidence that could justify including this functionality in SMETS 2?

    Answer: While we certainly are not in a position to argue with the research by the meter manufacturers that a threshold for a voltage excursion and a counter for the number of times an excursion occurred would cost money to implement, the conclusion seems to be oriented around the premise that generating an alert each time a fluctuation occurred would be needed. If one were to reframe the question and implement the suggestion above that the demand registers be collected by the communications hub every 10 seconds for demand response purposes, one might investigate keeping the threshold and counter in place and just forward the voltage excursion counter with the poll for counters by the communications hub. It would then be up to the correlation processor at the central site to determine if the voltage pattern were excessive given the review of the statistics collections when they are received. This is standard practice for performance management systems that use proxies like the communications hub and it eliminates the need for a meter to generate an alert each and every time an excursion occurs. The polling rate by the communications hub should be adjustable by the DNO. Some DNOs have indicated a desire to poll every 4 seconds under certain circumstances in concert with their belief that human reaction time requires a 4 second interval should such a correlation require a semi-continuous visualization of a situation.

21. If DNOs were permitted to access remote disablement functions, should control logic be built into DCC systems or meters? If the logic should be built into meters, should the logic be

specified in SMETS 2? Please provide rationale to support your position including estimates of the cost of delivering this functionality under the different options being considered and any evidence relating to safety issues associated with each option.

Answer: The question here is one of the viability of building policy logic into meters that could be provisioned and then directed by signals from multiple parties, and then continue to function in "off-line mode" when the WAN communications path is out of service.

There is certainly no problem with building a policy logic processor into a new communications hub where the interface to the WAN actually exists. But the flexibility of the meter itself to execute policy logic and yet remain inexpensive is the challenge.

The six application specific considerations seem to be the following:

1) The provisioning and activation of the service profile by the supplier of customer choice.
2) The option to participate in opt-in demand response programs for a more favorable price.
3) The need by the consumer to override an opt-in demand response commitment participation for exceptional situations.
4) The need for a DNO to curtail service for participating demand response sites.
5) The emergency need for a DNO to curtail service regardless of optional site participation.
6) The reinstatement of service when conditions permit.

The opt-in participation programs seem more oriented toward specific devices like EVSE, and temperature control and thus seem to not be oriented toward considerations 2, 3, and 4. Thus the discussion probably centers on considerations 1, 5, and 6.

Thus, the question becomes one of who does one trust to turn the power on and off?

For sure, the case can be made for the energy supplier terminating for non-payment.

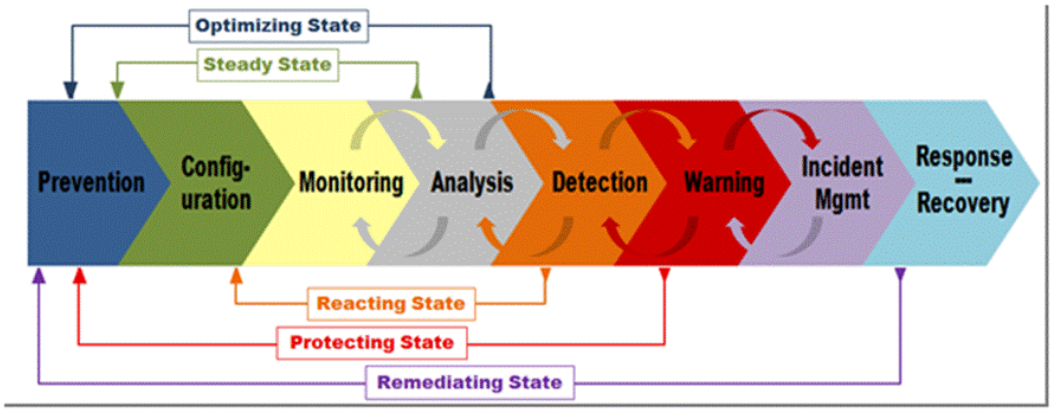
Yet for reasons of maintenance and emergencies, DNOs need to be able to disable supply (i.e. to perform work on their network) by isolating the feeder at the substation or at downstream junction point in the neighborhood. This option for curtailment can always be used regardless of the decision concerning an individual meter.

If the direction of the need is for the DNO to shut down service at a particular location for reasons of safety or some other eventual necessity, there are really three places to examine:

1) The meter itself

2) Some new device installed at the master breaker that can be remotely controlled by the DNO.
3) The communications hub

The communications hub can certainly be produced with complex policy logic as an on-site agent for both the energy supplier and the DNO to issue signals to either the meter or the new master breaker device, but the question is one of accountability for the policy logic. The question also is one of how the policy logic should operate under different operating modes. The TM Forum diagram below illustrates the different states in which a device can be, and depending on the signal from the energy supplier or the DNO, a slightly different set of policy logic may be required within each of the five operating states.



TM Forum Security Management Model

As long as installation operation by the energy supplier includes an activation step by the CSP that includes loading and verifying policy logic that can handle rulesets that support both energy supplier service states as well as DNO states, the communications hub could be the arbitrator and enable a simpler meter. However, as the interface to the WAN, the policy logic inside the communications hub will not be complete unless it includes logic that also takes into consideration the five operating states in the diagram above.

The final observation is that the policy logic needed to control the state of power enablement is fundamentally different from the policy logic needed to control the communications aspect of the communications hub. Generally these matters are simplified through the use of a separation kernel in the communications hub that separates the portation of the communications of the network from any application that was convenient to collocate in the device.

22. Do you agree that variant smart electricity meters should be specified in SMETS 2 and that the cost uplift for variant smart meters is similar to that for variant traditional meters? Please provide evidence of costs to support your views on cost uplifts.

Answer: Variant smart meters would of course necessitate a local control application on the HAN needed to handle external switches on the HAN as well as the internal switches for auxiliary load control. This would include boost button functionality to override any auxiliary load switching. The security on the HAN would dictate that end-to-end security be in place between these two elements for mutual authentication purposes as well as confidentiality of control command messages and responses.

Multiple measurement elements that allow concurrent tariffs on separate load circuits seem to have the same precautions in place so that the submeters and main meters are coordinated. If the communication of usage is the responsibility of the communications hub, then the authorized configuration of the submeters needs to be administered centrally with knowledge of the local configuration propagated to the communications hub so that data collection is properly controlled for reliable communications.

Costs uplift similarity should be a goal for the uplift if the communications hub is to assume this responsibility.

23. Do you agree that randomisation offset capability should be included for auxiliary load control switches and registers as described above? Do you have views on the proposed range of the randomisation offset (i.e. 0 – 1799 seconds)? Please provide evidence on the cost of introducing this functionality.

Answer: The randomization examples are good ones. The emerging effect of electric vehicle charging during the peak hour when people return home from work and then activate temperature adjustments will introduce an even larger concern in areas where dense concentration of electric vehicle owners exists. These are our findings thus far at the Pecan Street Project.

Thus it would appear that there are three algorithms that would be useful:

1) RTS style randomization for auxiliary load control switches activated via a schedule held in the metering system including the communications gateway.
2) Consumer choice (i.e. tumble dryers, pool pumps, and the like in response to a price change for time of day.
3) Choice of the DNO for round robin scheduling of EVSE chargers during periods of momentary stress during peak hours when users simultaneously engage charging.

Randomness appears to be a good solution for 1 & 2 above. Round robin appears to be good for electric vehicle charging so long as the individual chargers are individually controllable by the DNO's demand response system.

24. Do you support Option 1 or Option 2 for 'pairing' a CAD to the HAN? Please present the rationale for your choice and your views on the implications that these options have for the technical design of the solution.

Answer: Actually, the recommendation is for a combination of the two with some extensions.

Let us approach this from an examination of the provisioning and activation process in the first place.

1) During the beginning stages when an end user subscriber to energy services first moves in or otherwise makes arrangements to occupy a site. Arrangements are made with an energy supplier through some sort of application for service. During this time a check is made to determine the service location and the readiness of the facilities such that the energy service provider could immediately commence service, or whether some sort of physical installation needs to take place to enable the delivery of energy to the site.
2) Also, many types of private data are exchanged with the energy services provider to determine the creditworthiness of the subscriber to determine if the subscriber should be handled on a pre-pay or post pay basis.
3) At the conclusion of the pre-pay / post-pay decision and the understanding of whether an installation task needs to be scheduled, the basic course of action is that the energy service provider notifies the end user subscriber that service can be enabled and receives permission to enable the service with the subscriber's obligation to pay. This is the ideal time for the energy service provider to schedule delivery of the "welcome" letter and kit to the end user subscriber along with a one-time password to use to activate a CAD to control the activation of the service. The central association of the one-time password to the account and to the meter takes place before the welcome kit is released.
4) Part of the subscription process is the subscriber's election whether he wants a service provider CAD or prefers to use his own smartphone or tablet or PC to access the HAN using an app that can be downloaded from a popular app store. <This would necessitate providing that app via an appropriate number of choices.>

   Single purpose CADs could be sold by retail establishments and activated in parallel with the meter and communications hub on the premises by the end user subscriber.

   Note: Given the preponderance of users in the world today who own smartphones or tablets will prefer to use their personal device to interact with any item in their home as opposed to a "rogue" separate device that is inconvenient to use and subject to loss

or damage, there will be a strong affinity towards using their familiar personal tool of choice. This has two implications:

- The forecast of inventory of energy supplier CADs is extremely important and a balance needs to be achieved relative to retail provider's interest in stocking them.
- The limitation of using only ZigBee for the HAN instead of allowing the communications hub to also allow Wi-Fi for local access should be questioned. The consumer's CAD device of choice will be his smartphone or tablet if at all possible and Wi-Fi will inevitably be supported while ZigBee probably will not.

5) In order to activate the service, the end user subscriber must use the chosen CAD to choose a new memorable password along with a hint in case the subscriber misplaces his record of the self-chosen password. This is the same process as popular with the financial industry for providing security and privacy for access to financial records and other financial operations.

6) Other smart appliance devices purchased by the consumer subscriber on the HAN should automatically appear on the subscriber's "console" controlled by an app that operates on the communications hub that allows the subscriber to activate the device. The consumer should be in charge of making these selections.

7) Sometimes the consumer choice will be to also subscribe to a third party home energy service provider. This third party service provider would activate its service in much the same way as the energy service provider. As will be noted in the Security Section responses, in addition to communications hub network access, authentication, and authorization; each of these application-level services (be it from the energy supplier, the third party energy managed service, or any other) all need to observe the security arrangements for M2M application interconnection including confidentiality, integrity, and non-repudiation.

In terms of the objectives achieved:

- The ease of connection is maximized by allowing the end user subscriber to use his personal device of choice. (If the subscriber does not use a smartphone or a PC, the energy supplier approach is the only option.) The "consumer friendly" procedure should use procedures that are no more complicated than those on a television clicker or smartphone GUI best practices.

- Regardless of which approach is used, a technical assistance call center is needed to help users who are confused or who are having legitimate problems activating the service. If the HAN arrangement of meter and/or communications gateway is truly physically defective, a service call will probably be in order. However, to assist in the diagnosis, a diagnostic should be included on the communications gateway that,

with the user's permission, will allow the technician to "see what the user sees" and help the user walk through the activation procedure.

- Access from the CAD to the HAN (via the communications hub as the filter) should always be with secure communications described above and therefore mindful of the responsibility for both security and personal privacy). The communications hub should be able to "advertise" its services at the site, and then allow CADs to subscribe to those services by pairing in order to authenticate and authorize access to the HAN and to individual services on the communications hub.
- Noting that 50% of the meters are located in shared spaces, the communications between the meter and the communications gateway needs to be authenticated and encrypted.
- Most of the development time in the recommendations above seems to be on the provider of the communications hub as this is where the firewall is and the specialized access control and activation logic.
- Hidden in the discussion above are the multi-party responsibilities for device and application service authentication and authorization controls. Ultimately there needs to be a root of trust that allows agreements for energy suppliers to overtake one another in the service of subscribers.

Comparison of options:

- Option #1: Passkey
    - In some sense we are recommending elements of this as it is compatible with the subscription process. The difference is that there is no physical change on the meter or any physical button on the communications hub as the communications hub advertises its availability and then takes over the security arrangements. It is different in that the communications hub must interact with the central activation system to have access to other data about the subscription to the service that is internal and is never given to the consumer.
- Option #2: Remote Pairing
    - This is basically what we are recommending, except that rather than calling a person, the onetime passkey is used to authenticate the user and authorize the activation of the service on the communications hub. Part of that activation would include the retrieval of the service profile from the central system because that is where the order processing took place and the subscription and account records are held, including the Customer Information Number.

In fact, this is pretty much the same process as used by the device installer, except that it is an application service as opposed to the infrastructure device that is being activated.

This option avoids the problem of the SEC to be in the middle of the pairing operation as at the application level, the per-to-peer communications is directly between the energy service provider and the end user subscriber.

More should be discussed relative to the authorization process for one energy service supplier to overtake another, causing a disconnection from the incumbent energy supplier and a connect by the succeeding energy supplier. This is exactly the same as the local number portability scenario in the telecommunications industry, but it has not been mentioned in this consultation.

25. If Option 2 were adopted, do you agree that obligations should be placed on energy suppliers to support this process by submitting 'pairing requests' to the DCC on request from their consumers?

    Answer: Yes. The need for arbitration for overtaking energy suppliers discussed above results in this need.

26. Do you consider that other CAD installation options should be pursued? If yes, please explain the approach you favour and your reasons.

    Answer: Yes. See discussion above.

27. Do you agree with the proposal to include in SMETS 2 a specification for a PPMID, connected via the HAN, as described above?

    Answer: No. This device would be a complexity in view of the fact that the user already has a CAD device of choice for accessing the communications hub and thus indirectly to the meter. The UTRN one time code allows addition of credit from a designated vending agent.

    The argument against using the HAN to communicate credit data to the meter seems to be rooted in the concern that the security mechanism planned to be within the meter is inadequate to support the delivery of this function. The question to be asked here is why the meters that are eligible for pre-pay cannot be fitted with security arrangements good enough to prevent tampering with electronic credit and why the communications apparatus cannot be secured well enough to transmit electronic credit. More should be examined as to whether the communications hub can be secured enough to transact electronic credit and to securely interact with a properly secured meter.

28. Would including the capability to enable gas and electricity supply through a PPMID connected via (a) a wireless HAN or (b) a wired HAN meet GB safety requirements? What impact would including this capability have on the cost of smart metering equipment? Please provide evidence to support your answers.

Answer: This is more a matter of analyzing the costs to manufacture smart meter equipment that has an appropriate hardware security module chip in it for financial credit storage and device identification. The argument against such security may be rooted in the long term commitment for manufacturing runs of current equipment than in the feasibility of new meters. But with a large enough volume procurement opportunity, this is exactly what these hardware security modules are designed for.

Over 5 billion of these types of chips are produced every year. This is more a matter of introducing them to the power industry.

If this option is considered, chips that are certified as FIPS 140-2 level three are needed since we are dealing with stored credit here and tamperproofing is highly desireable. Specific features to be considered include:

- Differential power analysis attacks
- Voltage tampering attacks
- Temperature tampering attacks

29. Do you agree with the proposal that the communications hub should be specified such that it can support multiple smart electricity meters? How many smart electricity meters should be supported by each communications hub?

Answer: This question is somewhat akin to question #22 and the discussion regarding variant smart meters as far as the communications hub is concerned. The ability of the communications hub to support multiple interfaces such as are described is certainly not an issue. It is more the anticipated level of application space that is required.

As is anticipated, microgeneration and distributed energy resources will gain in popularity and thus two meters will become popular - but so will the complexity of the application in addition to the Feed-In-Tariff capability, Because the level of quality of power generated by alternative energy sources is not the same as bulk power generation, additional rules and regulations relative to the measurement of power and the synchronization with the grid are inevitable. This can mean additional control as a part of the microgeneration gateway device which may alter the information required by the metering element. The frequency of measurement and delegation of authority to deal with problems may be somewhat significant. This said, these considerations are more acute for the meter as opposed to the

communications gateway, except for the expanding need for more frequent measurements by the DNO.

If the need for implementing communications hubs with a long life before replacement is paramount, then the need for allowance for expansion in place is also paramount. This manifests itself in two ways:

1) The need for flexibility and safety of evolving application code and management policy code quickly will be much higher than in previous years.
2) The need for overprovisioning memory and processor power needs forecasting immediately even though the functions may be "out of scope" for the initial deployment.

An additional consideration for the features of the communications hub may be the inclusion of an additional features card to allow for contingencies. This expansion feature would allow for expansion of features such as

- RAM memory
- Persistent flash memory
- Processor
- Communication component for the WAN
- Communication component for the HAN
- Security components

There are many strategies for individual providers of these hubs. A physical change would necessitate a truck roll. But the emphasis should be on being able to maintain interface compatibility for the software running on the communications hub. As is popular with Apple products, the ability to install a significantly augmented device and then have an automatic system upgrade that preserves the previous environment will be worth enormous sums of money.

30. Do you agree that a specification for a HHT interface to the HAN should be defined? If yes, please identify the functions that this interface would need to support and the scenarios in which such functionality could be required.

Answer: Yes.

The supplier maintenance device would facilitate a variety of situations where the use of handheld terminals (HHTs) may be required to support their installation and maintenance activities, as described:

- Initial pairing of a meter to a communications hub

- Input of a meter point reference (MPAN or MPRN) as part of the installation process
- Input of an identifier for an auxiliary load control switch
- Configuration of meters in the event that the WAN is unavailable (either because connectivity has been lost or because the WAN service is not yet available at that site).

Given that meters will be switched between suppliers at change of supplier and that suppliers may change their meter manufacturers and meter operators (MOPs) to reflect commercial factors, we agree that a standard specification should be developed to allow a HHT to interface with smart metering devices via the HAN.

Any specification of the HHT interface to the HAN is dependent on the end-to-end security architecture and on clarifying how the preferred HAN standard (i.e. ZigBee SEP / DLMS) could support a HHT.

Chapter 5 Governance and Assurance of Security and Interoperability

31. Do you agree with the proposed approach to the governance of security requirements? If you propose alternative arrangements please provide evidence to support your views.

    Answer: Yes.

32. Do you agree with the proposal to establish independent assurance procedures for DCC and DCC users? Please explain your views and provide evidence, including cost estimates where applicable, to support your position. Comments would also be welcome in relation to the impacts and benefits of the proposed approach with regard to small suppliers.

    Answer: In that security is an end-to-end matter, the inclination to break up the system into independent roles because it becomes easier to administer seems fraught with risk. Is it too much to ask for a balance between both approaches? Role-based security may well serve the needs for certification, but interoperability can only be achieved with an end-to-end strategy. The Security Fabric Alliance proposes that the level of testing that you are contemplating here has both types of testing. This prevents an artificial pretense of false dichotomies in a zero sum argument.

33. Do you agree with the proposal that re-testing should occur at least at set intervals and more frequently when significant changes to systems or security requirements are introduced? Please explain your views.

    Answer: Yes.

34. Do you agree with the proposal to establish an independent security certification scheme for smart metering equipment? Do you have any views on the proposed approach to establishing a certification scheme or evidence of the costs or timelines for setting up such a scheme or submitting products for certification?

    Answer: Yes. The main delay in establishing the proposed testing organization is that of establishing the testing criteria. Also, in that we are all working against attackers that are other human beings that do not play by the rules, the requirements change at a brisk pace more reminiscent of the conduct of a war than a fixed set of academic problems. The introduction of new tests must take place at a brisk pace.

    We would suggest a distributed testing apparatus such that compliance testing could be performed daily as necessary. Also a distributed interoperability testing approach should be scheduled periodically, but at fairly short intervals to keep up with the pace of the problem being addressed.

    We would recommend the issuance of certified attributes upon successful test validation such that the attestation of currency can be automated right into the supply chain process and operational rhythm.

35. Do you agree that sanctions for non-compliance with security requirements should be included in the SEC? Do you have views on the nature of the sanctions that might be imposed?

    Answer: Sure. Revocation of the certified attributes or non-issuance of the certified attributes can allow the participants to police themselves, even at operations time.

36. Do you agree with the proposal to, in effect, extend the arrangements already proposed for SMETS installations prior to DCC operation, to all installations being operated outside DCC? Please provide evidence of the costs that might be incurred and the impact of this approach on small suppliers.

    Answer: Retrofit of security requirements into the legacy environment is the big issue on the table. A plan should be formulated that allows for a graceful transition whereby not all elements are secure all at once, but such that they can be adjusted over time without threatening the new devices that are secure. This of course will be the primary attack vector during the transition, and the esteemed opposition will learn new attack techniques within a few days of any new launch. Nevertheless, a transition plan is necessary to recover from the sins of the past.

    A transition path may include partial steps that lead to appropriate defenses over time.

37. Do you agree that interoperability is central to the development of a successful smart metering solution and that activities related to the assurance of SMETS equipment should be governed by SEC? Please provide views on the governance arrangements that would be appropriate for assuring interoperability of smart metering equipment.

    Answer: Absolutely. The views are part of the discussion above. Certification without interoperability leads to an impractical sense of security.

38. Do you agree with the creation of an 'approved products' list and the requirement on suppliers and CSPs to obtain, retain and provide evidence of appropriate certification should apply regardless of whether they intend to enroll the equipment in DCC?

    Answer: Yes. Use of the certified attribute system alluded to above is useful even if a CSP does not intend to enroll the equipment in DCC.

39. Do you agree that protocol certification (against a GB Companion Specification) should provide adequate assurance that a product will meet interoperability requirements? Please explain your views and identify any additional assurance testing that you consider to be necessary and the rationale for including such testing.

    Answer: This depends on what the GB Companion Specification says. Interoperability testing is different from certification testing. They should be "companion" specifications.

Chapter 6 Operational License Conditions

40. Do you agree with the Government's proposals to require energy suppliers to operate specific aspects of smart metering equipment functionality for domestic consumers? Please provide rationale to support your position.

    Answer: Yes, provided that personal privacy is reasonably maintained.

41. What are your views on the Government's proposals to require energy suppliers to operate specific aspects of smart meter equipment functionality for micro-business, but not other non-domestic, customers?

    Answer: The views seem plausible given the operating environment envisioned for a micro-business.

42. Do you agree that the licence conditions as drafted effectively underpin the Government's policy intentions for consumer operational requirements?

Answer: Yes.

43. What are your views on the Government's proposals for obligations to be included in the SEC for information to be made available to Network Operators and ESCOs via the DCC?

Answer: This will be fine as long as the arrangements for maintaining personal privacy are maintained. The Canadian approach using Privacy by Design appears to be well thought out.

44. Do you agree with the Government's proposals for the timing of the introduction of operational requirements? Please explain your reasoning.

Answer: Yes

Chapter 7 Next Steps

45. Do you agree with the proposed changes to the smart metering regulatory framework to reflect the CSP-led model for communications hub responsibilities? Are any other changes necessary?

Answer: Yes

46. Do you agree that the equipment development and availability timelines are realistic? Please give evidence.

Answer: Yes

47. Do you agree that SMETS 2 should only be designated when the Government has confidence that equipment to satisfy the new requirements is available at scale? Should a further period of notice be applied to ensure suppliers can manage their transition from SMETS 1 to SMETS 2 meters?

Answer: Yes to question #1 The second period of notice should be issued once the initial specification has been issued and suppliers have time to assess their own readiness.

48. What are your views on when responsibility for the SMETS modifications process should transfer from the Government to the SEC?

Answer: The milestone approach seems very appropriate.

49. Which of the options (standing sub-committee or non-standing sub-committee) would you prefer in relation to modifications to the SMETS?

    Answer: Why not both? A small standing sub-committee might need to be in place for the mechanics of advice, but given the nature of security attack, fraud, and the like, additional and very focused technical expertise may need to be brought in from time to time. The process for moving rapidly needs to be put in place before activation at an urgent moment.

50. Are there any particular areas of expertise that the sub-committee will need to fulfil its role, in terms of membership composition?

    Answer: Electrical engineering, distributed systems control, resilient RF communications, security, and personal privacy seem to be the key skills areas. Seldom do all 5 of these skills reside in the same person at the same time.