

Transporter on the withdrawal or decommissioning of a smart metering system, rather than 'reasonably practical' mentioned in H6.10. Similar requirements exist for Network Operators to be informed when new meters are installed on their network or otherwise brought in to DCC Service. This requirement is not explicitly stated within section H and should be added to ensure that Network Operators are aware of the existence of a smart meter, the meter variant installed, the SMETS version of the meter and the relationship between Device ID and MPAN(S) on the meter.

- In addition, we understand that Suppliers are able to update the MPAN(S) held on devices and in the DCC inventory. As Network Operators need to manage the relationship between MPAN and Device ID, in order to send service requests to, and process alarms from, Smart Meters the DCC or Supplier must be mandated to inform the Network Operator when this occurs.

Intimate Communications Hub Interface

Q9 Do you agree with our proposed text for the SEC with respect to the Communications Hub: Intimate Physical Interface? Please provide a rationale for your views.

Some of our members have concerns over making the ICHIS freely available as this may have the potential to increase security risk.

DCC Service Management

Q10 Do you agree with our proposed text for the SEC with respect to DCC Service Management? Please provide a rationale for your views.

In general our members agree with the proposed text. However, the rules governing the scheduling of planned changes should take into account that electricity distribution operations are heavily influenced by severe weather events. It is standard practice in the industry for planned changes to be avoided when severe weather is forecast, and work may be cancelled at short notice when weather forecasts change. The network operators will seek to make maximum use of DCC services to assist the restoration of customer supplies during and after severe weather. The same is true to an extent for the Communications Service Providers' networks.

Our members are satisfied that the proposed text follows the ITIL principles and sets out the provisions relating to implementation timetables for modification proposals, Release Management and maintenance of DCC systems. However, some suggest that the proposed text should be amended to include all ITIL processes, e.g. Problem Management. The SEC rightly recognises the importance of Service Management in line with the principles of the IT Infrastructure Library and therefore needs to include all ITIL processes.

Incident Management

Q11 Do you agree with our proposed text for the SEC with respect to Incident Management? Please provide a rationale for your views.

ENA members agree with the proposed text for the SEC with regards to Incident Management as it follows the principles of ITIL. It also includes content and responsibilities of the Incident Management Policy, development, maintenance and access to an Incident Management Control Log, concepts of a Major Incident and that the SEC panel will determine any disputes relating to Incident Management.

Self-Service Interface

Q12 Do you agree with our proposed text for the SEC with respect to the Self-Service Interface? Please provide a rationale for your views.

Our members agree with the proposed text for the SEC with regards to the Self Service Interface as it sets out the provisions for use and maintenance of the Self-Service interface. However, some of our members recommend that an additional requirement is placed on parties not to employ automated systems to submit multiple record requests. This is to ensure that the performance of the system is not affected by such actions.

Our members are also of the view that it would be useful for network operators to have visibility of information primarily designed for suppliers, especially for details such as meter type, meter model, firmware version installed and issues/ configurations associated with auxiliary load control.

In addition, for issues relating to the use of alerts to manage power outage response, it is important that parties gain access to information relating to the status of the SM WAN, and associated communications hub via the Self-Service Interface. Failure to make this information available will compromise network operators ability to deliver improved customer service by having access to power outage information provided by the smart metering system

DCC Service Desk

Q13 Do you agree with our proposed text for the SEC with respect to the DCC Service Desk? Please provide a rationale for your views

Our members agree with the proposed text for the SEC with regards to the DCC Service Desk as it provides a contact for Users 24/7 365 per annum which can be accessed by SEC parties and Users via telephone, e-mail or Self Service Interface. However, it is worth noting that the main intention of H8.19 is to ensure that an alternative email address and telephone number for the Service Desk are published by the DCC, so that parties may still contact the DCC Service Desk in the event that the normal contact methods are not available. Furthermore, some of our members comment that the proposed drafting in this section lacks clarity and appears to require 20 days' notice of the use of an alternative contact method.

Our members note there is no mention of a procedure to be followed, or when this will be delivered. So although our members we are in agreement with the principles as set out they look forward to further clarification on the processes and interaction between DCC Service Desk and DCC Users.

Service Level Agreements for Testing

Q14 Do you agree with our proposed text for the SEC with respect to the Service Level Agreements for Testing? Please provide a rationale for your views

ENA members agree with the proposed text for the SEC with regards to the Service Level Agreements for Testing as it sets out the measures for the performance of the DCC. The DCC will have to explain if it is under target and if it fails to meet the minimum requirement report on the steps taken to rectify.

However, while our members agree with the proposed text in principle, we are not sure that the information is complete. We understand that the Communications Service Provider agreements allow for significant deviation from the stated 60 second performance standard for alerts linked to outage management. The deviations could include the slow delivery of some alerts or the failure to deliver some alerts altogether. These arrangements do not appear to be documented in any of

the Technical Specifications and we do not believe that it is possible for the network operators to comment fully without this information.

In addition, given the key role that Service Providers play in the delivery of smart metering and smart grids, we propose that an additional requirement is added to H13.3. This would require the approval of the SEC Panel prior to any contract change that would modify the performance measures set out in the SEC.

Q15	Does the inclusion of DCC aggregate performance measures in the SEC, and the consequential reduction in future service charges, appropriately balance the need for the DCC to manage its Service Providers flexibly with the need for DCC Service Users to have a say regarding performance targets? Please give reasons for your answer.
-----	---

Our members do not believe that the inclusion of DCC aggregate performance measures in the SEC are sufficient for the DCC to manage its Service Providers flexibly. There should be a breakdown to each DCC Service provider to aid transparency and ensure individual Users are not being disproportionately disadvantaged. There are issues associated with the aggregate performance measures approach proposed and we are concerned regarding the possibility that some SEC parties may be impacted more by differing regional performance. In particular, those parties associated with poor WAN communications coverage in remote areas in Scotland and other parts.

In addition, our members also hold the view that it would add clarity if Testing was added to the list of performance measures in section H13.2.

Managing Demand

Q16	Do you agree with our proposed text for the SEC with respect to Managing Demand? Please provide a rationale for your views
-----	---

ENA members agree with the proposed text for SEC with regards to Managing Demand as it enables the DCC to manage the service capability by the Users providing six monthly forecasts. The DCC will provide a monthly comparison report for each User on the actual number of requests against the forecast which will show if the User has reached or exceeded the threshold.

It should be noted that Network Operators will have difficulty providing Demand Forecasts during the Suppliers' meter roll-out unless the Suppliers themselves provide an accurate geographical forecast of smart meter installations to be undertaken. Therefore, clarification is required regarding whether the proposals only apply after the roll-out is complete.

In addition, our members state that the DCC capacity limitations must also not be permitted to affect network operators' ability to deliver identified smart meter benefits especially in areas where there may be enduring issues with communications coverage.

Security Requirements

Q17	Do you have any comments on the security obligations set out in Section G of the SEC drafting or the way they are expressed?
-----	--

The security obligations documented in Section G of the SEC appear to provide a robust control environment which will safeguard the effective and accurate operation of Smart Metering.

However, our members hold the view that further work is required to understand the definition and practical extent of DCC User Systems to which the obligations will apply.

ENA members make the following comments regarding the Security Obligations set out in Section G and the definition of Security Check;

DECC accept the concept of a risk-based, proportionate response approach to application of the Security requirements. This must be clear in the wording of Section G.

It is our understanding that DECC do not expect all personnel/staff who have access to smart meter data to be covered by Section G, e.g. call centre staff. This must be clear in the wording of Section G.

It is our understanding that Users will be able to limit the scope of User Systems (as defined in the SEC) and therefore reduce the security requirements by reducing risk and ensuring a proportionate response. This must be clear in the wording of Section G.

The current definition of the DCC User System does not give enough clarity over what, if any, ancillary systems and users with access to the actual system (e.g. a party's smart metering head end system) are to have the SEC security obligations applied. In recent review meetings with the industry, DECC personnel have stated that it is not the intention that Section G will apply to a DCC User's backend systems which interface into a DCC User's primary system holding the trusted connection to the DCC.

Our members welcome this intention but the current version of the SEC does not provide the required clarity to enshrine the intention into actual SEC obligations. Such clarity could be made through enhancing the definition of 'Separation' to address what are adequate boundary controls between a DCC User's primary system and its backend systems.

Our members hold the view that security obligations should be realigned according to the user roles in order to be proportionate.

Our members also make the following points:

- Compliance should be a defined term in relation to the required adherence to the various ISO and British standards listed, in particular ISO 27001. The definition should state what level of audit and documentation constitutes 'Compliance'.
- DCC Users should be given a notification period for complying with any new versions of the referenced ISO or British standards. DCC Users cannot be expected to be 100 per cent compliant from the date of a standard's first public issue. Changes to such standards may not be known or accessible to a DCC User until after a standards issue. Compliance with any new or changed requirements within such standards would then need to be assessed and implemented.
- In relation to the 'security screening' obligations (G4), we need further definition of the extent of users encompassed by the phrase 'capable of Compromising the User System'. For example, we would be interested to know if such a definition includes authorised 'view only' users.
- G4.1 – this clause states that Users should be vetted to BS7858:2012 which includes financial status checks such as CCJ and credit checking which some of our members do not currently carry out. Is this level of financial checking applicable to Network Operators engineering operations?
- G5.13 – this clause states that Users information and security must comply with

ISO27001:2013, in previous Smart Meter documentation (presumably written prior to 2013) refers to ISO27001:2005. Is ISO27001:2013 the definitive standard to follow?

- Security Check Definition – UK Government vetting procedures can only be applied if you work on a Government contract or need access to Government classified information and have a sponsor. The vast majority of our member company employees do not normally have UK Government clearance. As private companies our members can do similar checks to the UK Government Baseline Personnel Security Standard (BPSS) which is to ensure Users hold valid Photo ID, have a valid NI number and have the right to work in the UK (work permit or residency status). Would this level of checking sufficient?

Q18 Do you have any comments on the appropriateness and / or the proportionality of the security obligations in relation to particular types of DCC Service Users and their role?

From a security perspective, there are three main areas where User Parties activity can impact the effective operation of smart meters:

1. Actions causing loss of supply
2. Actions causing financial impacts to User parties and customers
3. Actions compromising the security and integrity of smart metering equipment on customer premises

Electricity Distribution Network Operators have a single critical command, Update Security Credentials. Electricity Distribution Network Operators can only initiate actions which relate to 3) and then only to impact Electricity Distribution Network Operator non-critical operations. Other Users can initiate actions which impact all areas, e.g. Suppliers.

The impact of an Electricity Distribution Network Operator compromising the security and integrity of smart metering equipment on customer premises is limited to Electricity Distribution Network Operator functionality only and has no impact on supply of electricity, the customer or other user functions.

Security obligations applicable to Electricity Distribution Network Operators outlined in Section G should be risk based and be commensurate and proportional to the impacts of compromising the security and integrity of Electricity Distribution Network Operator functionality only.

Some of our members therefore suggest that a two-tier approach to User security obligations should be adopted.

1. Full scope of the security obligations to be a requirement for those users that can initiate actions causing loss of supply, financial impact and comprise the security and integrity of equipment;
2. A subset of the security obligations to be the requirement for those users that cannot initiate actions that interrupt supply or have a financial impact e.g. Electricity Distribution Network Operators.

Our members therefore suggest that a proportionate response using a risk-based approach for Electricity Distribution Network Operators security requirements would be addressed by role based access with strictly limited number of users plus stringent authorisation procedures (ring-fence key management). It is proposed that in due course, a full risk assessment containing a security threat assessment is used to validate this approach, with timescales to be agreed via the SEC Panel.

ENA members would welcome the confirmation that compliance with ISO/IEC/BSO does not mean certification.

Communications Hub Financing

Q19 Do you agree that the four additional provisions are proportionate responses to providing reliable and economic third party financing options for Communications Hubs?

Our members agree that the four additional provisions are proportionate responses to providing reliable and economic third party financing options for Communications Hubs. Separate charging provides visibility, while the contingency fund and the ability of the Authority to act in the event of the DCC defaulting should allow for competitive financing of Communications Hubs.

Whilst the communication hubs will be initially financed by the Approved Finance Party we assume that the day-to-day physical management of these hardware assets will be managed by suppliers in similar ways to how meter assets are managed by suppliers today (meter assets funded by Meter Asset Providers (MAPs)). There are issues in the way that meter assets are managed now, including how meters are handled and transported; unnecessary premature asset replacement; asset stranding and assets reported as faulty which are found to be sound upon testing. The application and recovery of charges to remunerate the Approve Finance Party should therefore carry appropriate signals and incentives for suppliers to manage communication hubs appropriately.

Communications Hub Services

Q20 Views are invited on the proposals in relation to Communications Hub asset charges and maintenance charges. This includes:

- Monthly Communications Hub Charge
- HAN Variant Pricing
- Monthly Maintenance Charge

Some ENA members suggest that this is an area that would benefit from economic modelling, once all the principal costs are understood. We believe that this is key to ensuring a cost effective and timely roll out programme.

Q21 Views are invited on the proposals in relation to charges following removal of a Communications Hub. In particular, views are invited on the proposals for no fault removals in split fuel households. Do you agree that any outstanding asset costs should be smeared across all users rather than being charged to the installing or removing Supplier when Communications Hubs that do not serve the second installer's equipment are removed from split fuel households? Please provide a rationale for your views.

Where a second supplier changes the original Communications Hub, not all our members agree that the most cost effective solution is to smear the costs across all commissioned Communications Hubs. This is an area that would benefit from a review after the first 18 months of operation.

Some of our members suggest that the related costs should not be smeared across all users so as to incentivise the installing or removing Supplier to ensure effective working practices.

Additional Comments

Annex 5: User Gateway Services Schedule		
	Issue	Comment
1	Paragraph 400. "All Services listed in this Schedule (including alerts) will attract an Explicit Charge pursuant to K7.5(b)"	Previous understanding from DECC was that alerts would be included in the fixed charge.
2	Service 3.3 Clear Event Log	Previous understanding was that Network Operator could not access this service.
3	Service 4.12 Read Maximum Demand Registers	Although various options around latency requirements were discussed previously with DECC, now that the available options have emerged as a 30 second "On Demand" service and a 24 hour "Future Dated" service there does not appear to be any reason why this service should not also offer an On Demand variant.