

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

Paper Reference:	SECP_108_1609_06
Action:	For Discussion

Panel Response to BEIS Consultation on ‘Delivering a smart and secure electricity system. The interoperability and cyber security of energy smart appliances and remote load control’

1. Purpose

This paper provides an updated draft SEC Panel response to the BEIS consultation on ‘interoperability and cyber security of energy smart appliances and remote load control, and its potential impacts to the SEC’. A copy of the draft response is included as Annex 1 to this paper.

The Panel is requested to review the draft response and provide any additional feedback by 23 September 2022, so a final response can be submitted following agreement of the Panel Chair by 28 September 2022.

A copy of the consultation may be found using the following link [BEIS consultation delivering a smart and secure electricity system](#). The Consultation closes 28 September 2022.

2. Summary Consultation Proposals

The proposals aim to unlock wider benefits of Energy Smart Appliances (ESA) and Demand Side Response Providers (DSRP), whilst at the same time protecting critical national infrastructure and creating a market that consumers have confidence to procure and take services. The proposals are aimed at the domestic and small non-domestic market. These are summarised as:

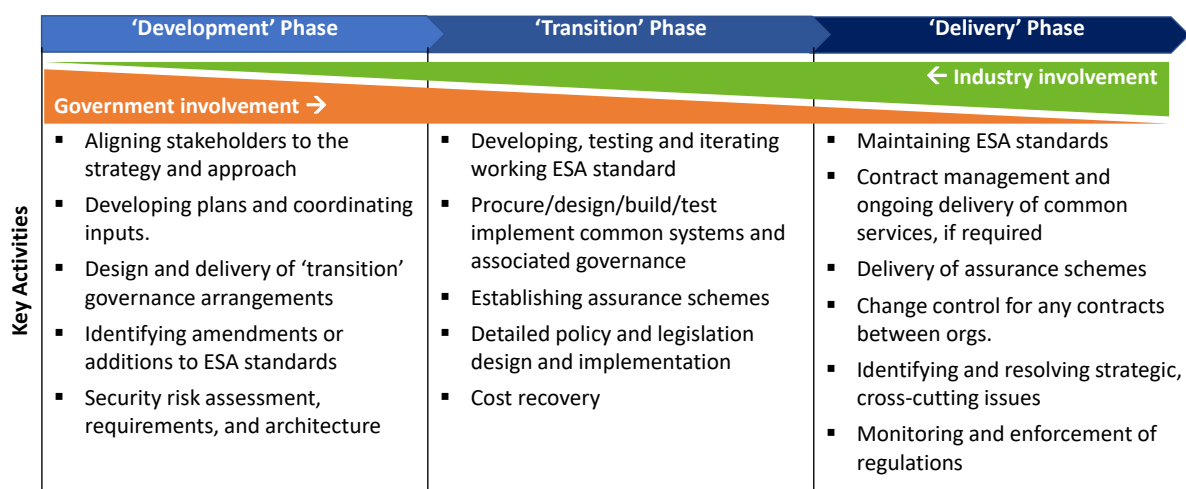
- ESA must have smart¹ functionality
- ESA must be able to receive and respond to Time of Use (ToU) tariff information
- ESA must be able to provide Demand Side Response
- Implementation of minimum standards for cyber security, grid stability and data privacy for ESA and Load Controllers (the organisations who will be able to control ESA, in effect

¹ Defined as: *the ability of the device to respond in real time to remote communication signals, using digital technologies, to deliver a service.*

potentially increasing or decreasing electricity demand) ultimately based on European Telecom Standards Institute (ETSI) EN 303 645

- Implementation of licence requirements for load controllers (controlling more than 300MW of load) and cyber security via NCSC NIS arrangements
- Adoption of interoperable Demand Side Response Standards based on Publicly Available Standard (PAS) 1878

BEIS has set up a programme to deliver the consultation proposals, similar to the governance framework used for the Smart Metering Implementation Programme. The consultation proposes that SEC is used as a Governance vehicle from the Transition phase onwards. The alternative would be to set up a separate not for profit body. The activities in each phase are summarised below:



3. Draft Response Development

Following SECP_107, SECAS has further developed the Panel draft response, shared this and discussed with wider SEC Parties, and updated again in response to feedback received.

With a number of the proposals having a security focus, the Security Sub Committee have also carefully reviewed the proposals and will also be submitting their own response to the consultation, with a focus on the security aspects. SECAS has liaised with the SSC to ensure no contradiction.

4. Recommendation

The Panel is requested to;

- Review the draft response and provide any additional feedback by 23 September 2022
- Approve the response to be submitted following agreement of the Panel Chair

Tim Newton

SECAS Team

09 September 2022

Annex 1 Draft Response

Peter Davies, SEC Panel Chair
Smart Energy Code Company Limited
8 Fenchurch Place
London, EC3M 4AJ

By email
SSESc consultations@beis.gov.uk

[28] September 2022

BEIS consultation: Delivering a smart and secure electricity system; consultation on interoperability, cyber security of energy smart appliances and remote load control

Dear Sir / Madam

The SEC Panel is pleased to provide a response to the recent consultation on interoperability, cyber security of Energy Smart Appliances and remote load control. The SEC Panel is supportive of the approaches outlined and will be pleased to work closely with BEIS to exchange views, share experience and to facilitate the development of the ESA and Demand Side Response (DSR) market.

Not all of the questions in the consultation relate to activities or actions that may be undertaken via SEC Governance. This response therefore sets out Panel views against the themes and areas within the consultation that have been identified with the greatest potential for SEC to assist with future development and implementation.

The consultation sets out topics and discusses potential resolution options. Without firm requirements to assess against, our response cannot contain a detailed assessment of the impacts on the SEC or detailed design solutions. However, we believe the response is at an appropriate level to enable BEIS to assess potential capabilities of where the SEC and its wider governance regime may facilitate.

The rollout of Smart metering, and the governance framework of the SEC, was originally envisaged as an enabler for wider “smart” activities. The Panel is therefore keen to build on, where appropriate, smart metering technical and governance capability to assist BEIS in its broader aims towards net zero.

The Panel response is set out below. The thoughts and views of the Panel have been distilled into four themes that we believe the SEC and its arrangements have the potential to support this programme. If there are any questions or you would like further clarification on any of the points below, please don't hesitate to ask.

1. Provision of Time of Use Data in a Common Format

The Panel, supported by its Sub Committees and SECAS, has extensive experience of managing devices to minimum specification and security/privacy standards. For example, parallels may be drawn between the proposals to publish Time of Use (ToU) tariff data in a common format, to that of the Central Products List (CPL) within the SEC.

Currently, devices must meet the CPL requirements set out in the SEC (Appendix Z) to be added to the CPL. Devices that do not meet the requirements of the CPL cannot be added by the Data Communications Company (DCC) to the Smart Metering Inventory and therefore cannot be communicated with.

SECAS manages entries to the CPL on behalf of the SEC Panel. The CPL is published on the SECAS website in a standard format for industry to view, in both technical and plain English versions. A similar approach could be developed for energy supplier ToU data and made available for ESA manufacturers. This could be overseen through SEC governance, so that any future changes are appropriately assured, documented and managed for industry. Lessons learnt through the operation of the CPL tool, from both a User and SECAS perspective would be applied, to ensure the process for updating information is as straightforward and user friendly as possible.

To set up a common format and register of ToU Tariffs will require discussion with all Suppliers and other Code Administrators/Managers to ensure agreement of the format, in addition to wider industry impacts being understood and resolved. In parallel, changes to the SEC would need to be raised, legal text agreed and implemented, and development of the SEC Website and working practices would need to be undertaken to accommodate the new data items. We do not foresee a need for DCC system changes for this service. The time to develop and get this service operational may take between 12 and 24 months, once BEIS confirm that SEC is the suitable place for this information to be managed.

The Parties potentially benefitting from this new service would not necessarily be those currently paying for SEC charges. As such, this new service will require wider consideration of the charging arrangements for this development work and ongoing use. The issue of charges is discussed further under point 4 of this response.

2. Energy Smart Appliance Interoperability Standards & Minimum Standards for Cyber Security

We agree with the proposal that ESA and DSR service providers meet certain cyber security standards. This is sensible given the potential risk to Critical National Infrastructure. In consultation with wider SEC Parties, views were expressed that any such standards should be mindful of potential asset stranding risks, to devices (including smart metering equipment) already deployed to avoid unintended consequences. Any standard and governance regime to assure it, should be mindful of the risk of technical obsolescence.

The SEC Panel, supported by the Security Sub Committee and SECAS, oversees security assessments of SEC Parties to ensure that the security requirements specified within the SEC are being observed. Comparison can therefore be made with the proposals for cyber security standards for ESAs. Privacy obligations within the SEC are also overseen by SECAS on behalf of SEC Panel, to ensure Parties adhere to the requirements appropriate to their role. This could be another important consideration if ESAs are entrusted to handle consumer and generator driven data.

The consultation notes further work is needed to assess the Publicly Available Standard (PAS) 1878 for ESA and the European Telecom Standards Institute (ETSI) 303 645 standard for cyber security. Initial discussions on this topic have been held by the SEC Panel Technical and Business Architecture and Security Sub Committees (TABASC and SSC respectively) to consider potential technical and security impacts for smart metering. The SSC is responding separately with views specifically on the security issues raised in the consultation.

Whilst there is reason to assume there may be a natural fit, there is also a requirement to consider the finer detail alongside the ability of the SEC and DCC Services to continue to deliver for Smart Metering. There may be different ways to manage the impacts on DCC services and the SEC, dependent on the level of DCC interaction. For example;

Option 1

BEIS may choose to develop a model whereby a Party could act in the role of the Responsible Supplier. This would require some assurance or the 3rd party to meet security requirements and potential changes to registration data for Change of Supplier purposes.

Option 2

Introduction of a new DCC User role for load control, employing full and specific security processes to protect the system for this role. This would be separate to the Responsible Supplier. This may take longer to implement with a need to make changes to smart metering systems and devices.

The TABASC considers that the DCC would be a good fit for many of the proposed measures, albeit accepting that there may be alternatives to DCC infrastructure, but it is not clear what these alternatives could be. Noting that until there is greater understanding of the future of ESA, or the way DSR will be offered and hence performed, TABASC is unable to confirm what, if any, technical smart metering changes may be needed. However, should there be an impact on smart metering systems, and therefore the DCC, the TABASC raised concerns over timescales for implementation given the current challenges facing the smart metering architecture. It was felt trying to incorporate more functionality may prove challenging for the DCC, especially at a time when DCC core services and fundamentally the level of service to its customers, should be paramount.

3. Common Systems – Communication Networks

Whilst the consultation is minded to not use DCC as a common platform, consideration should be given to the need and potential duplication in setting up a parallel set of services for this market segment. The final decision, may to some extent, be dependent on the outstanding security risk assessment. There may be potential synergy benefits for wider industry by amending the DCC licence to provide a common and secure platform for communications albeit, a “thin” or “lite” version may be appropriate.

Regardless of the use, or not, of the DCC as a common platform, the proposals to use Public Key Infrastructure (PKI) and Anomaly Detection Thresholds (ADT) is sensible and familiar to industry, as this forms part of the security solution for smart metering communication. The SEC Panel, DCC and SECAS are very familiar with issues with managing security practices such as the application of PKI and ADT.

The SEC, via its Security Sub-Committee, is also considerate of the latest guidance in security best practices as well as consideration of emerging threats to national infrastructure as guided by the National Cyber Security Centre (NCSC). Given these points, the SEC is a natural fit to govern this requirement.

It is not possible to provide a view on the level of resource required to facilitate and support any new common network from a governance perspective until the security requirements and risk assessment are completed. There are several “known unknowns” that will need to be fully understood and worked through to fully cost and provide an accurate view. For example;

- Level of Security standard compliance needed to be achieved but this should be at a proportionate level that does not stifle future innovation.
- Level of audits to be completed on ESA parties to ensure compliance with any proposed security model, commensurate with the level of risk.
- The development of ESA product specification(s) – lessons learned from Smart Metering are that any standard specification that is mandated, will need to be clear and remove any element of ambiguity to ensure interoperability across market participants. In addition the regulatory requirement should be proportionate to the risk it is seeking to mitigate for consumers. Parties support the need for a robust security network but need to see the risk assessment to ensure benefits and future innovation are realised.
- Consideration of System Traffic Management – the Bandwidth supported by any common systems will need careful consideration, including modelling the frequency of commands to and from ESA devices and potential implication for interactions with installed smart metering systems. If the DCC were to provide the communication platform, both the current and future demand for service and availability of that service, need to be fully understood. Industry developments such as Market Wide Half Hourly Settlement, changes to support balancing and settlement code uplifts and the potential addition of ESA devices (and associated commands), will require in depth analysis with DCC and its Service Providers.

4. Delivery Framework

The Smart Metering Implementation Programme (SMIP) has been working in tandem with SEC for several years, with work transitioning from SMIP to enduring SEC governance as services mature. The delivery framework proposed in the consultation is therefore familiar, and is a model the SEC Panel and SECAS would be comfortable operating. However, it should be noted that some of the reasons smart metering was deployed in the first place, included Demand Side Response market development. Some Parties are concerned of the need for another major programme.

Future development of the SEC to encompass a delivery framework for ESA and DSR regulations (consultation option 2) would provide industry with a single place within which all “smart” devices are managed. For example, new schedules and sections may be added to the SEC to detail the services provided and requirements for industry compliance, to facilitate the expected growth of this area of the market. Learning may be applied from the SMIP and SEC Panel from incorporating and managing newly designated sections of the code, and development of appropriate governance and oversight.

Changes to the SEC may be made via a proposal from a SEC Party (Modification) or these could be directed via BEIS under SEC Section X . Alternatively, a Modification could be directed from Ofgem.

It is under Section X powers that several Smart Metering Implementation Programme changes have been consulted upon and then directed to SEC. The SEC Panel would anticipate that this would be the preferred route for BEIS to direct changes related to ESA and/ or DSR governance.

The funding arrangement of the SEC and any potential new service delivery will need review and careful consideration, so that the costs for the set-up and operation of the ESA and/ or DSR services fall to those who use and benefit from them.

Alongside consideration of implications for charging, the wider SEC governance framework and constituency of Panel and Sub Committees, will also require a review. For example, if ESA's are required to become SEC Parties with a specific User Role, and contribute to overall SEC charges, these Parties would expect to be represented at the Panel and Sub Committees, where potential service quality and cost implications of any consequential changes to services are discussed.

Any new User Role would lead to new User Entry Process Testing requirements and assurance for SECAS to undertake, in addition to any security assurance techniques or potential audit requirements.

It is difficult to comment further on what specific changes to the SEC may be required whilst the security assessment is ongoing. However, if the review concludes that there will be services provided via the DCC, we anticipate that changes to the following sections may be required; Section A (definitions), B (Accession) C (Governance), H (DCC Services – including appropriate service level and service standard measurements, G (Security) , I (Privacy). If communications are to be delivered via the DCC (dependent on the options considered in section 3), there may be changes required to DUIS (DCC User Interface Services Schedule) and other subsidiary documents such as security Key Infrastructure and Anomaly Detection. In addition some Parties are concerned that any new service provision directed to be undertaken by DCC, does not deflect DCC, from focusing on its core functions ensuring these are running without issues before adding further to the DCC scope.

New sections will be required to cover any ESA standard specification, and as noted above, a review of charging will be required, which would result in changes to Sections J & K. Consideration should also be given to Testing of services ahead of go live and ongoing changes to those services. This may require amendments to Section P (Production Proving) and Section T (Testing Services).

An alternative would be to develop an approach, similar to the ALT HAN Services arrangements (SEC Section Z), whereby a separate section of the SEC sets out the specific governance arrangements for these services which may be managed outside SEC via Third Parties. This may be preferable if the DCC has no central role in delivery of ESA and/ or DSR services. For example, any such drafting may reference out to standards and a specification maintained by Third Parties with an overarching requirement to comply with appropriate elements of the SEC, and reporting to the SEC Panel for approval and oversight. However, for efficiency and simplicity, it may prove better for all Parties impacted for governance to be managed elsewhere if there is no direct Service provision by the DCC.

Any, and all SEC changes will need to be consulted upon and reviewed by wider industry and SEC Parties, ahead of any designation.

There will need to be a balance of enabling innovation, and the requirements on security and interoperability. Delivering secure and interoperable services through the SEC has been a primary concern. Lessons learned from smart metering and SEC operation is that delivering Security and Interoperability requires assurance processes, and common unambiguous specifications.

A governance model such as the SEC will need to preserve the security integrity whilst at the same time ensuring Interoperability and ease of use for market participants. This is not easy, and the SEC Modification process continues to evolve to provide that balance.

As stated, the intent has been to set out within this response, at a reasonable level of detail, potential options and ways in which the SEC and SEC governance processes may facilitate taking forward the proposals. However, it should be noted that, for any changes, a BEIS policy decision to utilise Smart Metering infrastructure and architecture is required, mandating load control alongside the regulatory changes discussed in this response. This may also have an impact on the overall smart metering rollout business case. The existing BEIS Impact Assessment underpinning Smart Metering is based on existing industry party compliance and participation (Suppliers, Network operators etc). Opening smart metering infrastructure to a new set of participants (albeit with specific development and set up costs) should be considered as an overall benefit or cost for consumers.

The Panel is keen to work closely with BEIS to further develop and discuss ways in which the Panel and the SEC governance framework may facilitate the growth of this important market sector.

Finally, we would note that BEIS and Ofgem Code Reform measures and DCC licence renewal is occurring during the same period that these new regulatory requirements and services are to commence. We would expect that any final decision ensures there are no unintended consequences.

If you would like to discuss any aspects of this response further, please do not hesitate to contact me on 020 7090 7755 or SECAS@gemserv.com

Yours Faithfully,



Peter Davies
SEC Panel Chair