The Future of Smart Charging

An Energy UK and BEAMA report exploring the approach to smart electric vehicle charging in the UK

BEAMA is the UK trade association for manufacturers and providers of energy infrastructure technologies and systems. Representing more than 200 companies, from start-ups and SMEs to large multinationals, members' products ensure low carbon energy and environmental services are delivered safely, securely and efficiently to UK homes, businesses, transport and grid networks.

Energy UK is the trade association for the energy industry with over 100 members - from established FTSE 100 companies right through to new, growing suppliers, generators and service providers across energy, transport, heat and technology. We represent the majority of the energy sector excluding networks and upstream oil and gas. Our members deliver nearly 80% of the UK's power generation and over 95% of the energy supply for the 28 million UK homes as well as many businesses. The energy industry invests £13bn annually, delivers nearly £30bn in gross value added on top of the nearly £100bn in economic activity through its supply chain and interaction with other sectors, and supports over 700,000 jobs in every corner of the country. The energy industry plans to invest £100bn over the course of this decade in new energy sources.

Introduction

The rollout of smart EV charging to domestic and small business buildings is well underway, and now that the smart functionality of chargepoints has been mandated by the Electric Vehicles (Smart Charge Points) Regulations 2021[1] we expect to see a rapid growth in smart charging not matched by other smart appliances. Indeed, for those with the ability to charge at home, smart management of energy is set to become a defining experience of owning an EV. For many people, the EV and its smart chargepoint is likely to be the first energy smart appliance they own.

Against the backdrop of rapid growth in EV uptake, Government and industry must agree ways to ensure optimal outcomes for consumers and for Great Britain's energy system. This is being undertaken under BEIS's Phase 2 Smart Charging work.

The Future of Smart Charging (FoSC) project was initiated by BEAMA and Energy UK in July 2021 in response to recommendations of the Electric Vehicle Energy Taskforce Technical Working Group. It seeks to help all stakeholders, including Government, understand the implications for industry and consumers of identified options for delivering the interoperability and cyber security of smart charging devices and systems while providing required levels of data privacy and grid stability.

This report is a summary of outputs from workgroup discussions over the period October 2021 to May 2022. We would take this opportunity to thank all the organisations involved in the process, who engaged in an open and frank discussion that will accelerate delivery of an approach to smart technology, including realising the potential benefits for consumers.

Energy UK, BEAMA, and our respective memberships will continue to work collaboratively as the smart standards continue to develop under the Government's ongoing Smart Secure Energy Systems work programme. This work will set the scene for smart devices and tailored tariffs and services to be delivered to all UK consumers, enabling the sector to deliver decarbonisation at most efficient cost to consumers, and setting the scene for a nascent market to develop into a globally leading sector delivering growth, jobs, and export potential.

We welcome engagement from other stakeholders as we continue to engage on this important but highly complex area of reform, essential to establishing the best possible outcomes for consumers, for the energy system, and for the UK.

[1] https://www.legislation.gov.uk/ukdsi/2021/9780348228434/contents

Contents

Section 1: Background and purpose of this report

The progress toward smart charging standards has been a technical process involving a wide range of stakeholders. The core context is set out in this chapter, setting the scene for Energy UK and BEAMA to establish a targeted group to enable open discourse and accelerate progress.

Smart charging regulations

Government consulted in 2019 on proposals for smart charging, seeking to require smart functionality at EV chargepoints sold or installed in the UK. It published its response to the consultation process in 2021, stating the intention to mandate minimum device-level requirements for private chargepoints, signposting further (Phase 2) proposals during 2022, and mooting the sharing of chargepoint location and energy data with certain parties.

Government also sponsored the British Standards Institute (BSI) to develop and publish two publicly available specifications of particular relevance: PAS 1878[2] and PAS 1879[3], which together define an energy smart appliance (such as a smart EV chargepoint) and a demand-side response (DSR) system. PAS 1878 imposes high level requirements on the communications between the energy smart appliance (ESA) and the customer energy manager (CEM). These requirements relate to cybersecurity (especially authentication and encryption) and an information mode compatible with the fully defined interface between the CEM and the DSR service provider (DSRSP).

Together these documents form the context for Industry's consideration of Government requirements and consumer expectations for device and service interoperability, for cyber security and data privacy, and for grid stability. In order to coordinate this process, Energy UK and BEAMA established the FoSC project.

Industry considered the options for implementation and likely implications for manufacturers and service providers of these requirements, including the smart 'architecture' of the domestic or SME building. This 'architecture' refers to the smart elements within the buildings and the electrical and communications connections between them. The architecture will be dependent on the interoperability, cyber security, privacy, and grid stability outcomes expected of it.

The FoSC project looked to set out the core considerations across smart architecture, and also considered what forms of governance would be most appropriate and effective to deliver the intended outcomes for consumers and the energy system.

Views expressed in this report take as a starting point, given the state of the market, an assumption that any decision on an interoperability requirement would be unlikely to be implemented before 31 December 2025, but that the introduction of other requirements would be subject to Government consultation.

[2] https://www.bsigroup.com/en-GB/about-bsi/uk-national-standards-body/about-standards/Innovation/energy-smart-appliances-programme/pas-1878/

[3] https://www.bsigroup.com/en-GB/about-bsi/uk-national-standards-body/about-standards/Innovation/energy-smart-appliances-programme/pas-1879

Future of Smart Charging Project

The project's primary objectives were:

1. To establish, in partnership with Government, specific minimum requirements that any smart charging system must meet, notably in relation to achieving interoperability, cyber security, grid stability and data privacy; and

2. To explore the viability of a framework or frameworks for smart EV charging in domestic and small business buildings that delivers system and user outcomes that meet Government requirements and meet industry expectations.

Under BEIS's Phase 2 Smart Charging work, they will look to mandate these minimum requirements by the end of 2025.

As a secondary objective, the project considered whether and how to undertake an assessment of the compatibility of existing industry standards and specifications, including PAS 1878 and PAS 1879, with required outcomes and of their suitability for use in a wider framework for a secure and interoperable smart charging system.

Deliverables

The project aimed to deliver feedback directly to Government, and to set out those core considerations into a report that would support an industry-led technical framework to deliver Government's smart charging requirements (as per Phase 2 of its smart charging work). This framework should be coordinated with the increased electrification of heat and be consistent with other requirements of smart energy management as low carbon technology at the demand side increases in popularity.

The purpose of this report was not to draw definitive conclusions regarding policy. Instead, its intention is to help to advance the debate and inform ongoing industry discussions which support the best outcomes for all stakeholders impacted by smart charging developments.

Contributing organisations

This report is the product of the FoSC Working Group, which consisted of members of the BEAMA Electric Vehicle Infrastructure Group and the Energy UK Electric Vehicle Working Group. These two groups, and other members of BEAMA and Energy UK, were also consulted in the development of the report and its findings represent, as far as possible, a collective view of the two organizations. However, no statement or claim should be ascribed to any constituent organization or individual. The report authors have strived to represent the breadth of perspectives, noting both divergence and convergence of views.

BEAMA and Energy UK thank the Department of Business, Energy and Industrial Strategy (BEIS) for its support for and engagement with this project. This report also benefitted from input from groups within the BEAMA Flexible Energy Systems sector, comprised of its Smart Metering, Consumer Energy Data, Smart Buildings, and Electric Vehicle Infrastructure groups, and from the Energy UK Electric Vehicle Working Group, and Smart Metering Delivery groups.

Those wishing to learn more about the activities of these groups are encouraged to contact Jeremy.Yapp@beama.org.uk or Yumann.Siddiq@energy-uk.org.uk.

Section 2: Wider Context and considerations

The challenges of regulating for smart charging can be considered through more than one lens, including approaches centred on the system, the consumer, the market, and the required outcomes or expected solutions. We have recorded the initial thoughts on these contextual considerations that informed our discussions.

General context

EV charging is our focus…

This report has been written from the perspective of the provision of EV charging, based on discussions with a cross-industry project team including manufacturers and providers of EV supply equipment (EVSE) and of the electrical and communications connections required for EV charging; of cloud services and energy management systems; of DSRSPs, energy suppliers and chargepoint operators (CPOs); and with input from National Grid ESO.

… but many of the discussions will be equally relevant to other smart appliances

We acknowledge that the EV chargepoint is not the only appliance using a significant electrical load that can be controlled or managed smartly. Therefore, although the focus is on EV charging, many of the observations and conclusions of the report can apply equally to other appliances. Furthermore, the system for EV charging described in this report will need to allow for the smart management of electrical appliances

System context

The system around smart charging is complex

There are numerous impacted actors: including the established EV supply equipment (EVSE) industry, vehicle manufacturers, existing and future DSRSPs and energy suppliers, Distribution Network/System Operators (DNOs and DSOs), third party intermediaries, and the Transmission System Operator. Further complexity is introduced through parties such a CPOs, who can also interact directly with the chargepoint.

There are multiple use cases to consider: CPOs' activities will normally focus on publicly accessible chargepoints, but there are already use cases being developed where CPOs are using smart charging protocols, for example OCPP, to deliver innovative propositions such as dynamic Time of Use Tariff (ToUT) for EV charging for domestic customers and Type of Use, in which the electricity tariff is different (usually less) for an EV chargepoint than for other appliances[4].

The EV chargepoint is one of several potential (flexible) loads in a system: users may want to manage the building or system as a whole. This means the EV charging will need to be integrated into the electrical and communications management, alongside all other

[4] See for example see https://www.ovoenergy.com/electric-cars/anytime

	loads such as the heat pump, battery, microgeneration assets and other energy smart appliances
Smart charging is different to smart metering	The EV smart charging system is a complex network of participants, interactions and transactions and is markedly different from domestic smart metering, which may be inappropriate as a benchmark for comparison or baseline operating model.

Consumer context

Consumer experience is already a core consideration of existing solutions	Alongside system security, stability, and resilience it is equally important to consider the end consumer who owns or uses the EV. They will interact with the chargepoint potentially multiple times per day, particularly if their chargepoint provides or is connected to additional features such as energy monitoring for the whole home, load balancing with local renewable generation, and smart or optimized charging. In most cases, the consumer will use an app that they will expect to be easy to use and highly responsive; undue latency in the response causes frustration and disconnects the consumer from their product and, consequently, compromises their willingness to allow a third party to manage the charge of their EV – a fundamental requirement if smart EV charging is to deliver the expected benefits. The increasing levels of competition in this market are already delivering benefits for consumers by pushing suppliers to offer the best possible outcomes to their customers.
We are not 'designing from scratch'	EVSE manufacturers have invested heavily in software development and servers to manage the interaction between the app and the EVSE, and to provide additional services such as the requirements of the Electric Vehicles (Smart Charge Points) Regulations 2021.5 Any proposed regulations should build on these systems by introducing security without adversely affecting the consumer experience, without devaluing the previous investment, and without unduly compromising existing business models and systems.
EV infrastructure can be the core of an expanded system of ESAs	The infrastructure already in place for EVs is likely to form a key part of any future domestic DSR interoperability framework, which is likely to include a suite of smart-controlled electrical appliances, not just the EVSE.

Market context

The market is nascent but changing rapidly	Requirements for DSR services are already driven by network operators, National Grid, Ofgem and Elexon, and successful regulatory outcomes for smart charging may depend on

[5] https://www.legislation.gov.uk/ukdsi/2021/9780348228434/contents

	finding the right balance, in the short term, between delivering high product standards and supporting new innovations and system evolution. Our view is that at this stage in the development of modern technologies and markets it is important to focus on outcomes rather than extensive and tightly defined standards.
UK participants may wish to operate globally	EVSE manufacturers, vehicle manufacturers and CPOs operate in a global market. It is therefore important that any requirements that are Government mandate for Great Britain do not restrict the sale of products to other countries or introduce excessive complexity in the manufacture and distribution of the products. If GB requirements deviate substantially from international standards and solutions, this would increase costs and potentially make GB a less attractive market for manufacturers and/or providers.
The UK market should be attractive with limited barriers to entry	Excessive regulation or an unstable policy or regulatory environment may reduce the overall attractiveness or ease of entry of the UK market to new EVSE manufacturers. Appropriate use of standards may enable interoperability and smooth the path for DSR services, but over-zealous standardization at a formative stage of this sector could hamper industry efforts to innovate and risks creating barriers to entry for new players.

Solution context

We are considering issues without defining solutions	This report is not intended to define an agreed solution to the complex issues around smart charging given the importance of enabling continued innovation and development of solutions. It should be seen as another stage in the ongoing engagement between industry, Government, and other stakeholders to reach a robust and workable solution.
Ongoing enduring engagement is necessary and welcome	The nature of developments in low carbon technologies means we must embrace incremental but constant change over the coming decades. Rather than a single regulatory intervention, we must expect and support an ongoing evolution of regulatory requirements that encourages efficiency and innovation in solutions development.

Initial working assumptions

To manage the breadth and direction of group discussions, we set some early expectations relating to each of the four requirements pillars:

1. We expect requirements and expectations for **interoperability** between devices and systems to broadly align with those set out in PAS 1878 and 1879

2. We expect **cyber security** requirements to be determined during 2022 by Government; in the meantime, we will aim to deliver a high degree of confidence in device-level and system-level cyber security, in accordance with the intentions of Secure by Design policies and, where appropriate, PAS 1878 and 1879
3. We expect **grid stability** requirements to be determined by Government, the Regulator, Distribution Network Operators (DNOs) , NG ESO, and flexibility service providers: the project will endeavour to describe a home architecture that delivers data and responsiveness in a way that meets the needs of stakeholders who contribute to the stabilization and management of the electricity grid
4. We expect **data privacy** requirements to align broadly with GDPR, but to be applicable at device level; that is, devices will be required by standards to support that level of data privacy

Section 3: Discussion and assessment of approach

This section sets out the core approach taken, before setting out the core options discussed by the FOSC Working Group.

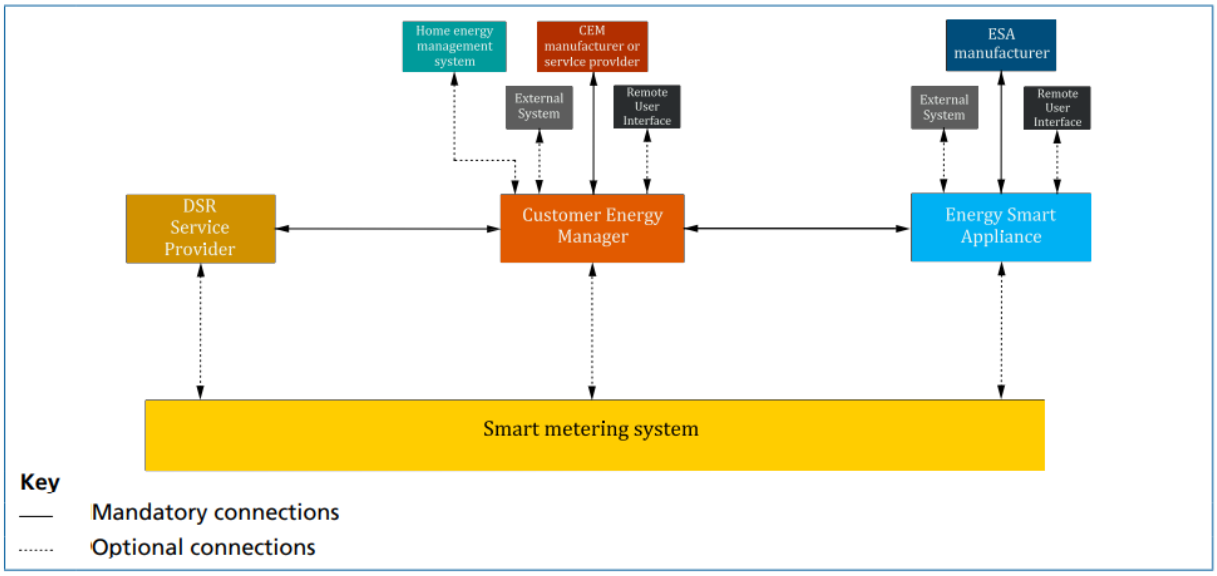
Interoperability

This report takes its definition of interoperability from the PAS 1878 and 1879, as follows:

[The] ability of an ESA to work seamlessly across any appropriate DSR service operated by any authorized system player, including allowing a consumer to switch an ESA to a different DSRSP at any time and maintain DSR functionality[1]

This can be represented as follows:

Figure 3 – Representation of system level CEM–ESA energy flexibility architecture with separate CEM/ESAG



Resulting Project Question

The project considered which minimum requirements EVSE interoperability should satisfy to ensure the best possible consumer experience, while avoiding unnecessary cost increases or constraints to market development.

Assessment of PAS-style interoperability

The project group agreed with the PAS definition of interoperability due to the benefit of this architecture being consumer ease in switching service provider or energy supply, while continuing to receive an uninterrupted service, fulfilling the specified minimum requirements relating to DSR and other services.

Key requirements and recommendations for further thinking

1. **Government should not define how the experience of interoperability is delivered.**
2. **The process of switching to a different DSRSP should be simple and transparent and should not require a site visit to replace or adjust the EVSE.** These requirements will satisfy the best possible consumer experience.

3. **Future work should resolve whether different mechanisms for interoperability are incompatible** and should give recommendations on how industry can cohere around a universal approach.

Cyber security

Smart EV charging will be subject to certain cyber security requirements to be set by Government. For the purpose of this project, two aspects of cyber security were considered as exemplars of an industry-wide approach; services relating Public Key Infrastructure (PKI) and Anomaly Detection. These were chosen for their clear implications for central systems, which would take a significant length of time to procure and make operational.

PKI Problem statement

Government will require smart EV charging to be subject to a PKI service that enables issuance and management of the digital certificates. This will deliver confidentiality, integrity and non-repudiation of the data that moves between access points or across systems.

There are no internationally recognized standards for PKI management, though secure communications on the internet provide a good reference model for how PKI works in practice. Until such a standard is published, it will be necessary for some level of governance to be established.

A PKI has been defined for ISO 15118, which focuses on the communication between the vehicle and other actors. However, there are other communications links that also need to have a secure communications channel, which in turn need to be covered under an end-to-end security system. It is worth noting that there may be multiple trust anchors or root certificates installed on the vehicle for different roles, including certificates from the vehicle manufacturer and Mobility Operators (MOs). Therefore, there are already multiple PKIs in play and multiple processes may be required to pass these certificates around the different actors.

Resulting project question

The Project considered three generic models for a PKI service and scrutinised each in terms of its likely benefits (how much security it would provide to the system) against likely costs and time implications, as well as other factors.

Options assessed

1. **A centralized body** providing PKI which manufacturers and service providers must use, similar to the requirements of IEC 15118
2. **A central body as a root certificate authority (CA)** with multiple entities authorized by this central body to act as sub-CAs
3. **A licensed/approved vendors model**, where manufacturers and service providers can choose which PKI they use, providing the PKI provider is authorised for use by central governance

Option 1: centralized body

Advantages

⊕ **Easy administration**	Simplicity in administration when creating, issuing, tracking, revoking, and auditing certificates

⊕ **Straightforward quality assurance**	Ease of quality monitoring of certificate processes and quality, due to greater efficiency and oversight from a single body.
⊕ **Speed to market**	Faster market access for new products and services, and ability for them to interoperate with other providers more easily. (Note that this has not been proven to be the case for interoperability at a more general level.)

Disadvantages

⊖ **Higher go to market costs**	May require international manufacturers to support their products with firmware specific to the UK/GB. Additional overheads and excessive complexity in the manufacture and distribution of products for those selling globally and needing to support and maintain multiple firmware versions for different territories.
⊖ **Single point of failure**	Higher risk to overall system security should the centralized body be compromised, make an error, or be subject to a cryptographic threat that targets its unique properties.
⊖ **Cost of co-ordination**	Additional industry-wide coordination cost when certificates change or are revoked, because a centralized system responsible for the generation of all certificates (roots and intermediate certificates) may require the DSRSP, CEM, CSMS and CS (and possibly EVs) to be involved. The centralized body must be able to issue certificates which tie in with a manufacturer's production processes. (For example, in SMETS, certificates have to be bought upfront in a batch and then installed in the smart meters; if this were applied to chargepoints, **the EVSE could become dependent on an external organization** to provide certificates).
⊖ **Concerns over equivalent existing arrangements**	An official centralized body for ISO 15118 does not currently exist. The private monopoly which runs the *de facto* centralized ISO PKI is a subject of concern for some in industry, and there are several industry-led projects (for example those led by SAE and CharIN) to address these concerns which propose an open and interoperable PKI.
⊖ **Resistance to innovation**	Experience with the smart metering system and its governance gives rise to concerns that a central PKI body may have less incentive to innovate and less reactive to industry needs. This would be a concern given the pace of the rapidly changing EV industry.

Option 2: root CA with sub-Cas

Advantages

⊕ **Potential for outsourcing**	A service provider or manufacturer could derive an intermediate certificate from the UK Root Certificate and use it to create subsequent certificates for different products or locations. This would produce a company-specific OCPP server certificate created from the company-specific Root Certificate (which is in turn derived from the UK Root). This would provide a high degree of interoperability, as the company-specific OCPP server would be able to communicate with all charging stations regardless of their manufacturing provenance, as long as they were loaded with the UK Root certificate.
⊕ **Technical simplicity**	If a manufacturer sells a specific product to a third-party CPO and installs the UK Root certificate into the charging station, there is potential to communicate with any OCPP server, suggesting a solution which may be technical straightforward compared to other models.

Disadvantages

⊖ **Costs of coordination and interoperability**	This model may stipulate that each manufacturer or central system provider can have their own intermediate CA, and as such it may pose interoperability challenges or increase the coordination effort required.

Option 3: approved-vendors model

Advantages

⊕ **Competitive pricing landscape**	By allowing for the selection (from an approved list) of PKI vendors, this model will likely deliver lower prices than a price-controlled monopoly, ultimately better benefitting consumers.
⊕ **Overall system security**	With multiple PKI providers, the EVSE may switch to an alternative vendor if the primary vendor is compromised.
⊕ **Potential for good governance**	If governed correctly, with an approved testing regime for certifying and verifying that devices are compliant with the standard, certain risks associated with sub-CAs can be mitigated. - While the seamless transition of PKI certificates will be required to support Change of DSRSP, processes to be learnt from are existent in Change of Supplier or Change of Tenancy in smart metering, however each carry complexity and cost.

- Multiple certificates could exist to support different interoperability if a standard process is defined on how certificates from different PKI vendors can co-exist, detailing how to obtain and verify certificates, consistent across vendors.

⊕ Resilience to poor governance at the Root level

This could be achieved if an independent industry body licences or approves root certificates, ensuring meaningful competition and space for innovation (though at the cost of duplicated Root infrastructure).

Disadvantages

⊖ Associated costs of change in protocol

Today chargepoints only have one trust anchor where a root certificate can be installed. With multiple root certificates, the CPO must either store these certificates or there must be a process to replace certificates on the devices. There is currently no suitable solution to manage multiple trust anchors.

If this cannot be accomplished without a site visit, the expected interoperability requirement will not be met.

⊖ Complexity

Each PKI impacts components used in the EVSE, in particular the cryptographic hardware or processors capable of supporting cryptographic communication.

Lower power processors may not be able to support more complex protocols; there is a risk of limited compatibility between the multiple PKIs and the chipset used in the EVSE, which is especially important in the context of a global shortage of silicon devices and rapid inflation in the price of many microprocessor families.

⊖ Cost of operational uncertainty

Numerous questions remain about how such a model would operate: how companies will be notified of a new authorised provider, when a provider is removed, and how the list of authorized providers is maintained.

- Complexity is added with each new authorised provider as the cloud would need to hold a new derived intermediate certificate.
- It is not yet clear who would administer the process of device connection to a server, by indicating which root certificate (or intermediate certificate) to use.

If different certificates are required from different vendors in a single device, the level of manufacturer complexity will increase considerably, especially when unnecessary delays occur in accessing vendors during busy periods. The process would need to be fully automated and to operate transparently.

⊖ **Challenging quality monitoring**	This model risks diversifying supply, compromising quality and challenging overall coordination without appropriate governance.

Implications of multiple PKIs for interoperability

Multiple PKIs introduce an extra complexity by requiring cross-certification to enable trust of the other CA-roots (trust anchor management). It could be more challenging to deliver interoperability and security in this scenario because multiple authorities may require greater resources at device level for trust anchor storage and processing. Complexity exists with all models, but multiple PKI create the potential for multiple integrations, thus increasing the complexities through development. These concerns have not been quantified, however, and may be possible to address through standards.

DSRSPs and PKI providers would need to establish a methodology for transferring trust between themselves in the event of a change of DSRSP. This complexity could bring significant cost and resource challenges. Furthermore, any errors in the process could lead to risk of device stranding and subsequent warranty claims and impacts to the end consumer. It is worth highlighting here that there is no currently defined mechanism for interoperability or switching between DSRSPs. Therefore, transfer of trust is just one functionality that needs to be implemented.

Further research is required to determine whether the expected level of complexity, which is acceptable to some stakeholders, would be manageable with a scalable energy management PKI and/or would be outweighed by the benefits of this model.

Anomaly detection problem statement

Anomaly detection is a mechanism for identifying remotely communicated messages as being anomalous by virtue of either their content or their quantity. Regarding the EVSE, the AD function's aim to prevent (load affecting) attacks on the CNI-impacting communications, rather than detecting them after they have already been actioned. As such, the AD function must monitor any command, generated by the consumer app or DSRSP, before it is relayed to the EVSE, therefore acting in real time and responding within milliseconds if performance of the app or DSR service is not to be adversely affected by AD system latency. It will be essential that the AD function has an extremely high availability.

Resulting project question

The project considered two models for Anomaly Detection (AD), scrutinising their benefits and costs.

1. **Central function** providing anomaly detection.
2. **Licensed/approved vendors model,** whereby service providers can choose which AD service they use, providing the AD provider is authorised for use by central governance.

Identifying what the AD function is intended to detect and what type of action is intended in response will be critical in designing the solution. The model must not introduce any noticeable delay in the transmission of:

- Requests for a mode change or power variation from the customer app or DSRSP to the EVSE manufacturer platform (or other system) that manages these requests
- Commands from the EVSE manufacturer platform (or other system) to the EVSE

Assessment of central AD function

The assessment included the following core considerations of a central AD function:

- **Existence of a single point of failure:** If control actions must be pre-authorized by the AD function, then this would be the obvious target for a cyber-attack.
- **Quality of operation:** Consideration of the appropriate methodology and governance for a single entity to oversee the operation and solution centrally.
- **Potential for increased investment in reliance and recovery:** The scale of the central operation could allow for deeper investment in resilience and recovery to meet the Service Levels and Response Targets, which may not be as consistent nor as tight if multiple smaller providers are delivering these services.

Upon agreement that a less centralised approach will not satisfy Government security requirements, and no indication that this approach would be cheaper, simpler or faster to deliver, absent of any Government indication to suggest otherwise, the FoSC project declined to more closely investigate options for design, implementation and management of this model. Focus shifted to consideration for future work in design of an effective centralised AD system.

Key requirements and recommendations for further thinking

1. **Cost recovery:** A system for cost recovery is required for providing the AD function in both development and operational terms.
2. **Agreement on purpose of anomaly detection:** Further thinking should establish whether the function is intended to:
    - Identify attacks on individual chargepoints, a single substation or bulk supply point, or at a national level
    - Identify an attack on a single CPO or EVSE manufacturer system
    - Identify actions that could cause disruption to the power grid by switching multiple devices, or whether a Denial of Service (DoS) attack is also in scope, given that such an attack could prevent a DSR action

    Following this, a process for Industry and Government to agree on anomaly thresholds should be discussed.
3. **Agreement on post-detection actions:** These may include:
    - how different actors are informed if an anomaly is detected
    - The actions they are expected to take when notified
    - The governance arrangements for notifying a central agency of a DoS attack on an individual company's infrastructure

Grid Stability

Smart charging may present certain risks to the stability of the grid. For example, when multiple chargepoints respond (switch on or off) to a price signal at the same time, sudden steps in load can arise causing issues for local network operators when balancing the system at a national level.

Problem statement

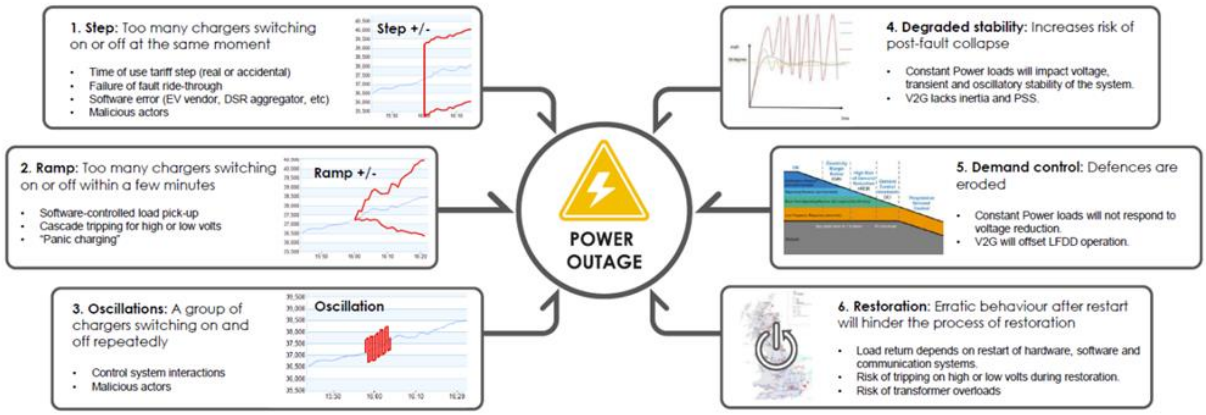
As EV chargers present certain risks to grid stability, certain mitigation efforts will also fall under the responsibility of the CPO and will likely include specifying devices with capabilities that limit the potential size of the steps experienced and result in a controlled ramp rate.

Resulting project question

Which chargepoint-specific solutions best protect the grid from identified risks while not adversely affecting the market, with minimal cost to the price of a charging unit?

Options assessed

The diagram below summarises the main risks to the grid that could be caused by EV charging, and were assessed by the FoSC project:



Source: Resilient Electrical Vehicle Charging: "REV" (Sygensis for National Grid ESO, Feb 2022)

It was recognised that each grid risk (effect) may have multiple potential causes and consequentially each cause may lead to its own potential solution (mitigation). For example, consider the following:

Effect	Cause		Potential solution
Step	1.	Loss of communications	Firmware level (randomisation)
	2.	Malicious attack	Cloud level (protections)
	3.	Price signal(s)	Supplier level (co-ordination or regulation)

It was noted that a communications outage is the most likely near-term risk to the grid given current levels in number of EVs, with the effect of a step change.

Furthermore, it is not immediately clear whether all risks and potential solutions are best the responsibility of chargepoints to mitigate or, for instance, by suppliers via co-ordination of tariff settings, and/or by networks and the grid via additional engineering developments. Though the latter are not the focus of this report, their suitability under a range of mitigation actions must be acknowledged by Government when identifying which solutions fall on chargepoints in particular.

Finally, when introducing short-term solutions it is important to delivery immediate benefits to the system and consumers; but medium- and long-term solutions will need to be developed and deployable at a later stage to more appropriately manage an ever-growing ESA-user population.

Key requirements and recommendations for further thinking

1. **An evolutionary approach to solutions is more appropriate than establishing day one mitigation requirements.** The need to mitigate sudden coordinated changes in EV demand will increase rapidly as the number of EVs and participation in flexibility grows. As such, the 'power' of a fixed mitigation measure will likely be insufficient by the end of a product's life in 10-15 years.
    - Policy can either set the measure to be excessive from day one to ensure proportionality years later or set the measure at current necessity levels and allow evolution, including change of, solutions. The latter will save cost in the long term.
2. **Randomization is the short-term solution.** The Government has already mandated this function in smart chargepoints, but Project members indicated that it should be considered a near–term solution, implemented with appropriate consideration for consumer experience.
    - Randomization is an effective near-term solution to avoid issues of system loading synchronisation, a critical requirement to mitigate communications outage scenarios, for example – where a charger automatically returns to standard charging mode, and may need to endure in case a consumer has not selected a DSR regime.
    - The functionality must exist at device (firmware) level owing to the risks relating to communications outage, but it may also exist in the Home Energy System and/or at hardware or Cloud level.
3. **We recommend a process of modelling, mapping, and trialling to identify and map responsibility for long-term solutions.** Solutions to grid stability risks are complex to identify. Modelling should help industry understand the effectiveness of potential mitigations against a number of EV growth and grid stability scenarios. Small scale trialling, for example deliberate block loading in a controlled setting, may indicate whether a particular mitigation has been effective. And live testing on solutions is essential because of the way device behaviours differ between laboratory and field.
4. **Industry will need impact assessments and a commitment from Government on engagement.** Any additional requirements placed on chargepoints inevitably place an increased cost on the unit, the impact of which must be assessed as part of a full cost-benefit analysis. It is essential that Government provides an ongoing commitment to collaborate with key stakeholders to develop these medium- and longer-term solutions.

Data Privacy

EVSE collects and shares substantial amounts of personal data. UK GDPR (which includes provisions from EU GDPR) and the 2018 Data Protection Act are the primary regulatory frameworks governing the present EV charging data privacy environment.

There was some agreement within the Project that application of the outcomes of GDPR to current ESAs and supporting systems would achieve an appropriate level of data protection for consumers. However, because GDPR applies to organizations, its direct application to ESAs (devices) or systems does not seem possible. The Project therefore recommends further joint working to investigate the practicality of applying the principles or outcomes of GDPR to ESAs, perhaps by reviewing scenarios or use cases to identify those in which sufficient protection for consumers would not be achieved.

Further, proposals are required to describe an implementation regime and the governance of data privacy for ESAs. It would not be enough simply to point to GDPR and its outcomes and consider that they afford consumers sufficient protection and access to redress.

Problem statement

Future requirements on smart chargers relating to the technical specifications discussed in this report, on interoperability, cyber security, and grid stability, will all demand increased data sharing with new actors and therefore may introduce new data privacy risks. Although GDPR remains the base from which future data privacy standards should be set, new technical requirements may reveal regulatory gaps or consumer protection concerns that are not in scope of the existing framework.

Resulting Project Question

With the expectation that current UK GDPR may fall short of the full scope of data privacy required in the new smart charging environment, where and how will these likely gaps in the framework arise?

Options Assessed

The Project's approach was to outline advantages and disadvantages relating to potential options for meeting new cyber security requirements while we await further government clarity, so new data privacy gaps relating to cyber security have not been assessed. The Project makes the following recommendations regarding interoperability and grid stability requirements to inform thinking on potential gaps.

Key requirements and recommendations for further thinking

1. **Cyber security functionalities and requirements:** Industry should consider forming a dedicated Working Group to test (in field and lab settings) solutions to cyber security requirements as they are articulated by Government. These solutions should be mindful of integration and interoperability challenges.
2. **Data privacy:** Further work is needed to address the challenges of applying to devices and systems data privacy requirements currently on organizations.
3. **Integration and communication:** Much more work needs to be done in real-life and field settings to identify the communications protocols most suitable for smart energy management, and to agree the role of each element of the system (especially the relationships between the HEMS, CEM and ESAs).
4. **Review of the Smart Meter Data Access and Privacy Framework:** The increased granularity of personal data necessary for interoperability requirements warrants review of this framework as an effective starting point.
5. **Data sharing on the state of charge may be beneficial to understand the technical limits to flexibility that the individual charger can provide.** The smart charger's power and energy levels, and where these sit within the range from maximum to minimum help inform how far it can be turned up or down, and how long it can be held at that level.
6. **Data sharing of the locational tag:** Should a locational tag be attached to all the information leaving the charger?
    - It would be helpful for anyone using the flexibility from or information about a charging EV to know where on the network it is connected. In fact, many of the services a DNO or the ESO might want to buy are only valuable if we know the location - E.g., devices measuring and responding to changes in frequency. Presumably this is to provide frequency response and reserve services to the ESO, those services will have no effect if they are located behind a network constraint, and therefore of little value if they come with no locational data to test this.

- We can see a scenario where some of the more difficult flexibility products for EV charging to access might start first at larger charging locations, for example in parking lots or business properties. For reasons including the economies of scale (due to both number of vehicles and speed of charging), the ease of getting locational data with high confidence, and that they may to be connected to higher voltage parts of the network, avoiding low voltage network constraints.

Appendix: Summary of recommendations

Interoperability and Cyber Security

1. Government should not define **how** the experience of interoperability is delivered, but the process of switching DSRSP should be **simple and transparent** and should **not require a site visit** to replace or adjust the EVSE.
2. Future work should determine the **compatibility of different interoperability mechanisms** in order to recommend a universal approach.
3. Government should support an industry consortium that will develop a detailed implementation to meet known requirements and interoperate with common standards.
4. Separately, Industry should consider forming a **dedicated working group** to test solutions to cyber security requirements as they are articulated by Government.

Grid Stability

1. An **evolutionary approach to solutions** is more appropriate than establishing day one mitigation requirements.
2. Randomization is the **short-term solution** and must exist **at least at firmware level.**
3. We need a process of modelling, mapping, and trialling to **identify and map responsibility for long-term solutions**.
4. Industry will need **impact assessments** and a commitment from Government on **continued engagement**.

Data Privacy

1. Further work is needed to address the challenges of **applying current data privacy requirements to devices and systems**.
2. More work is needed in real-world settings to identify the **communications protocols most suitable for smart energy management**.
3. The increased granularity of personal data necessary for interoperability requirements warrants review of the applicability **the Smart Meter Data Access and Privacy Framework** in its current form.

DISCLAIMER

While the information herein has been compiled in good faith, no warranty is given or should be implied for its use and BEAMA and Energy UK hereby disclaim any liability that may arise from its use to the fullest extent permitted under applicable law.