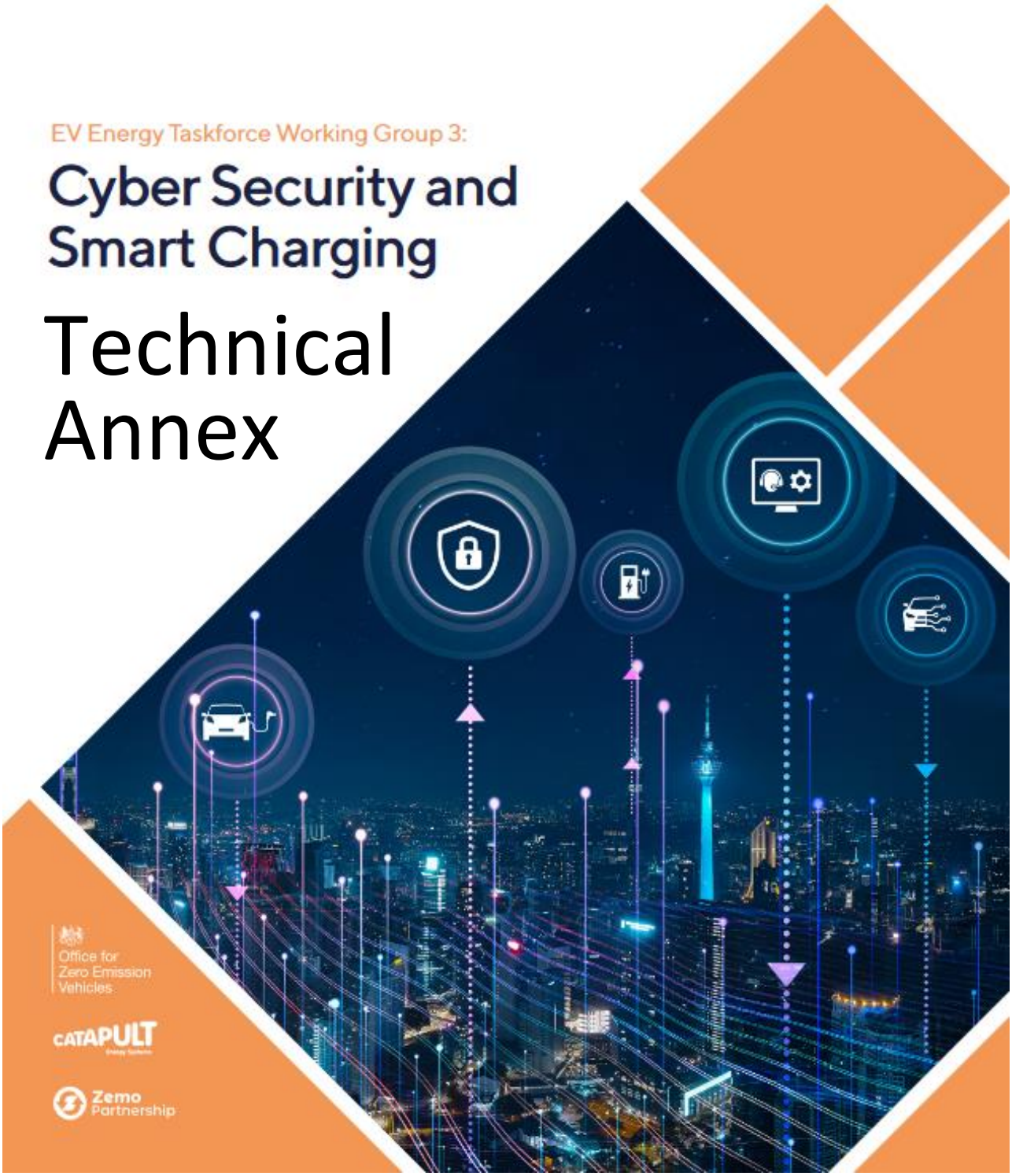
energy taskforce

EV Energy Taskforce Working Group 3:

Cyber Security and Smart Charging

Technical Annex



Office for Zero Emission Vehicles

CATAPULT

Zemo Partnership

Contents

1. Introduction and background

1.1. Aim

As a working subgroup of EVET2 WG3 representing key EV charging market participants the aim was to develop a technical specification (TS) for EV chargers to accelerate Great Britain's transition to electric vehicles. The 'optimum' outcome for the GB smart charging system is still to be determined, however this report is intended to help develop the criteria by which candidate solutions may be judged. Further iteration on candidate solutions is therefore required.

1.2. Objectives

1. Accelerate the transition to electric vehicles by developing policy holders' objectives into a technical specification, agreed by a representative range of stakeholders;

2. Inform industry consensus on EV smart charging technical specifications;

3. Develop a worked example for how smart charging could work in practice, expressed in terms of a technical specification;

4. Develop outcomes-based technical guidance in the interests of consumers and their needs;

5. Achieve logical derivations of consumer needs, policy principles, high level requirements and high-level architecture in that order;

6. Consider a range of solution options including smart, non-smart and mixed approaches;

7. Phase the work as follows to enable the complexity to be developed in stages:
    a. Phase 1. Residential Off-Street charging
    b. Phase 2. Residential On-Street charging
    c. Phase 3. Workplace and destination charging
    d. Phase 6: Roaming across international boundaries
    e. Phase 4. Optionally, detailed technical specifications to enable implementation
    f. Phase 5. Optionally, a proof of concept

8. All deliverables to be made publicly available

These objectives have been partially achieved. While a range of market participants were consulted, we have been unable to receive input from vehicle manufacturers. Policy principles and use cases have been assessed to a reasonable level of detail, although a detailed technical specification for the candidate architecture has not been completed in the time available. We propose that the assessment described in this report is used to inform further work to develop a detailed technical specification for the candidate architecture. As intended, the work was restricted to residential off-street parking (Phase 1 only.)

Part way through the study, it became clear that PAS 1878 was unlikely to be mandated in the near future. Therefore, while we have identified the associated PAS 1878 use cases, analysis of these use cases has not been carried out.

1.3. Process overview and report structure

The proposed approach was to:

1. Consult with a range of policy stakeholders to establish the important policy principles;
2. Identify the use cases (commands and messages) that will be of relevance to EV charging;
3. Assess the use cases to identify their impact on the policy principles;
4. Develop candidate architectures (smart, non-smart and mixed);
5. Assess the candidate architectures and make recommendations for future adoption.

The process overview describes how policy findings and use case analysis have been synthesised into the candidate architecture. This derivation of policy findings, use case analysis and architecture synthesis is developed in this report according to the process flow shown in Figure 1 along with references to the relevant sections in this document where the process outputs may be found.

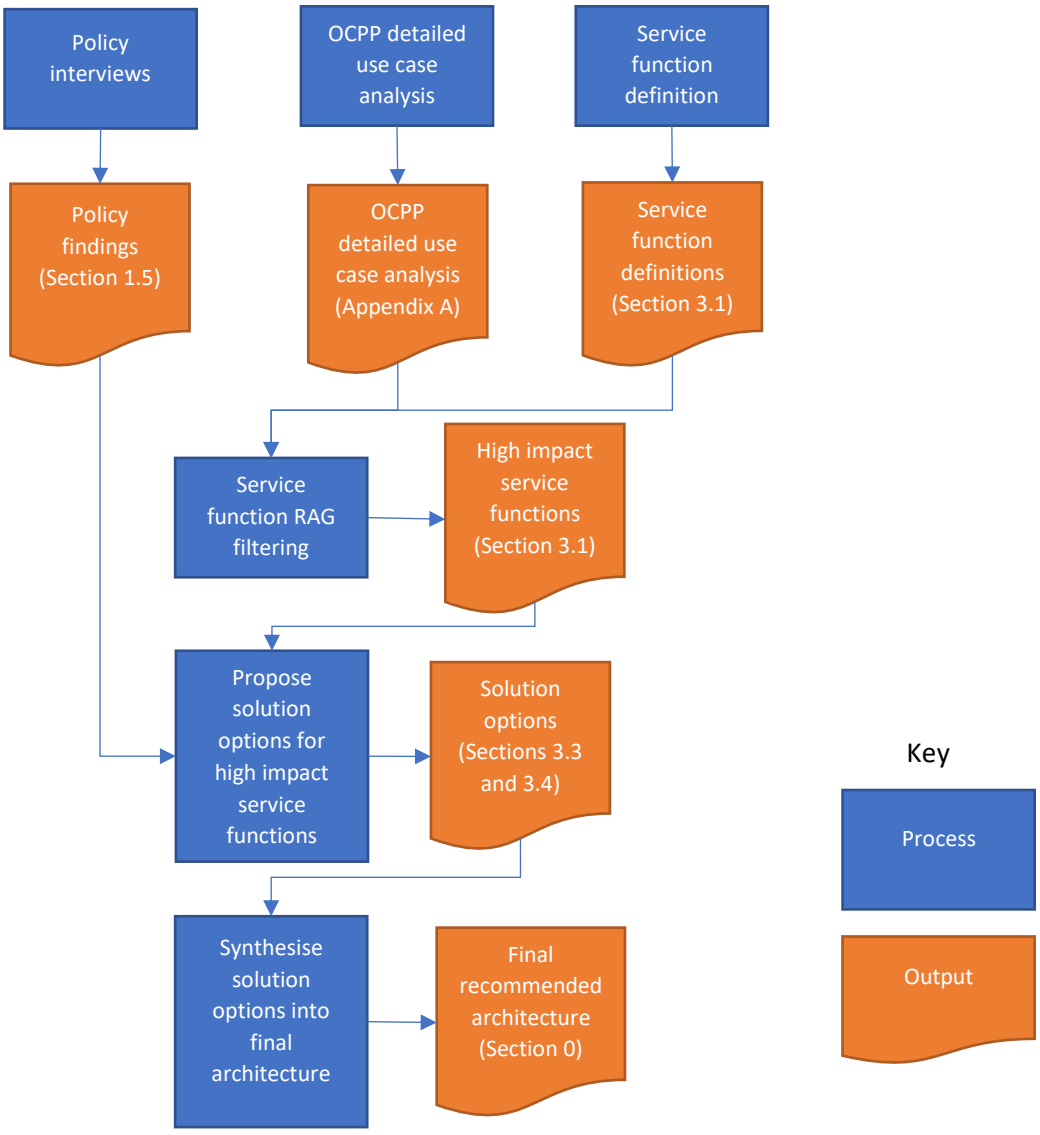


Figure 1. Process flow and document guide to outputs.

1.4. Stakeholder consultations

We received input from a range of industry stakeholders on both policy principles and also system functionality and architecture. It should be noted that while a wide range of input was received, this does not necessarily imply that all conclusions are supported by all contributors.

Policy stakeholders consulted included:

- BEIS / OZEV
- NCSC
- Citizens Advice
- ENA

Industry stakeholders consulted included:

- Pod Point
- Flexitricity
- Centrica
- Kaluza
- Landis+Gyr

Some stakeholders expressed reservations regarding the use of the smart meter system as the main transport mechanism for EV charging messages due to perceived issues of latency, its monopolistic position and ability to deliver innovative, customer-orientated services.

In terms of interoperability, one CSMS contributor suggested that the financial impact of mandating specific protocols (e.g. OCPP) could be significant (although not quantified) whereas the alternative approach of ad hoc integration of non-interoperable protocols, although requiring significant investment, may only be required on the occasions when a CPO ceases operating.

1.5. Context diagram and definitions

Figure 2 shows the various actors defined for use within this analysis.

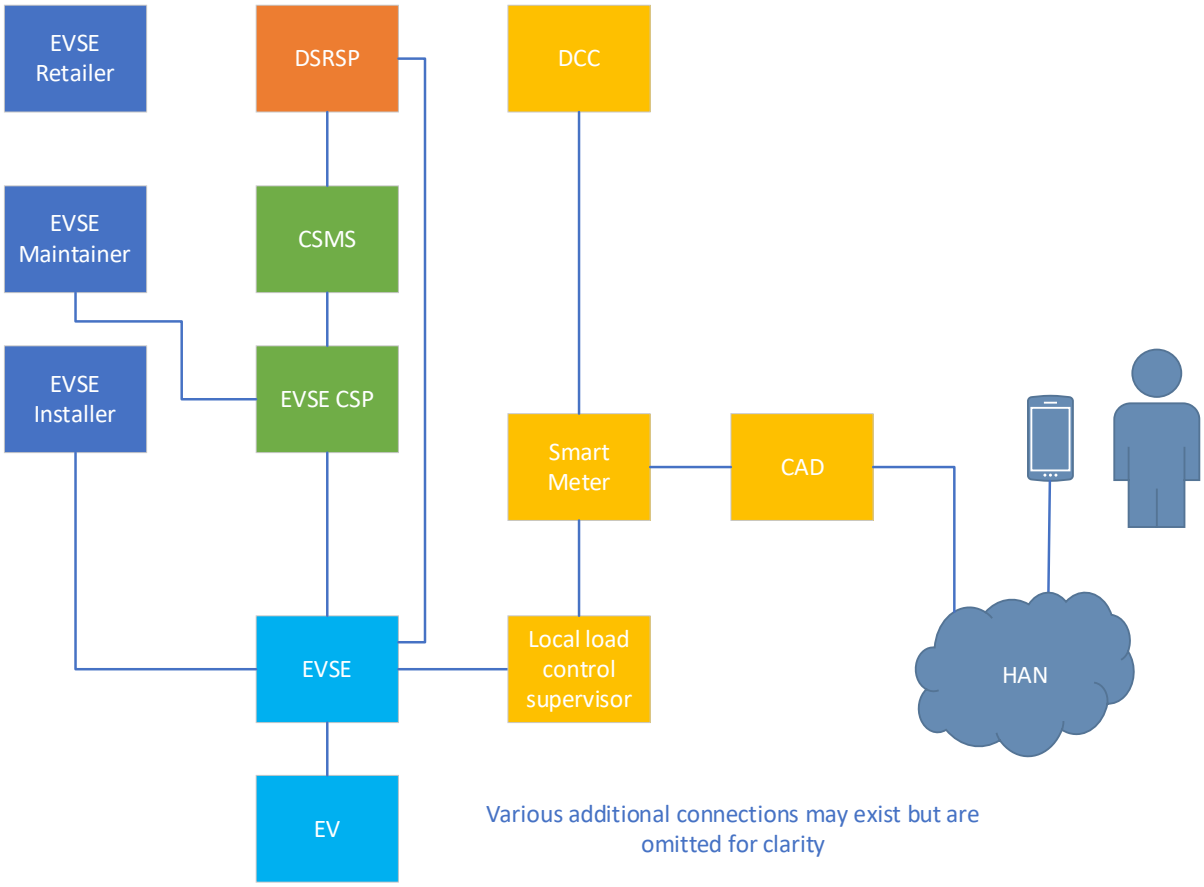


Figure 2. Context diagram of actors used in this report

The following actors are defined:

- EVSE: Electric Vehicle Supply Equipment
- EV: Electric Vehicle
- CAD: Consumer Access Device
- DCC: Data Communications Company
- HAN: Home Area Network
- Local load control supervisor: Secure means of arming the EVSE ready to accept a load control trigger
- Charge Station Management System (CSMS): Provides management and control of the EVSE;
- EVSE Communications Service Provider (EVSE CSP): Provides the WAN communications service between the CSMS and the EVSE, likely to be either broadband or cellular;
- Demand Side Response Service Provider (DSRSP): Uses EVSEs to provide demand side related energy management services to regulated electricity market participants;

- EVSE Installer: Responsible for installing the EVSE;
- EVSE Maintainer: Responsible for maintaining the EVSE through life, particularly in relation to firmware upgrade.

Although the customer energy manager, defined in PAS1878, is not explicitly shown on the diagram, it may be useful to consider this component residing between the CSMS / DSRSP and the EVSE. Its function is to provide protocol translation between the service provider and the appliance. As this report focusses on EVs rather than energy smart appliances in general, the CEM translation function is omitted for clarity.

1.6. Out of scope

The following topics were deemed out of scope of this work, either due to the time available or doubt that they would be fruitful areas for investigation:

- The electric vehicle itself is out of scope of this report, due to an inability to regulate for its requirements through the Automated Electric Vehicle Act;
- Protocols related to roaming and settlement between service providers;
- Communications protocols other than OCPP (see section 3);
- DNO load control of EVSE;
- Physical installation of the hardware;
- Details of consumer user interface;
- Energy smart appliances other than EVSE.

While the electric vehicle itself is out of scope of this work, it is recommended that further work is done to consider the security and interoperability implications of direct EV control. This capability is available on the market today and, if left unaddressed, has the potential to undermine any attempts to regulate the chargepoint for security and interoperability.

This work is done in the absence of any detailed threat analysis to justify the security-related policy findings and any subsequent security recommendations that may be included as a result. It is assumed that this work is being carried out elsewhere.

2. Policy principles

This section of this report aims to provide inputs from key stakeholders concerning their priorities for different aspects of provision of EV smart charging and energy flexibility (Demand Side Response) within a domestic off-street setting.

Multiple interviews were carried out with BEIS, Citizens Advice (to get the consumer view) and NCSC. These interviews were based upon a questionnaire to give insights to the following sections of work around use case analysis and design.

These findings have fed into the standards-based candidate architecture design and enabled the work to identify shortcomings within standards that need to be addressed to meet likely new requirements and regulations before wide-scale adoption of flexible EV smart charging and DSR services can commence.

The stakeholder views expressed during the interviews were initial, informal views for guidance only and not intended to be definitive statements of policy or representative of policy decisions. Future solutions and regulation development should elaborate and justify in greater detail how the policy findings have been arrived at.

2.1. Policy sections examined

The questionnaire was structured around the policy objectives and key areas for the design of the smart charging system in Great Britain. These areas were:

- Cyber Security
- Grid Stability
- Data Privacy
- Interoperability
- Consumer Protection

These topics were not looking at consumer-facing benefits or features, as it was assumed that the market will largely determine these; they were rather looking to establish the likely key areas of policy and regulation the system will need to be designed around to meet its objectives for Great Britain.

All questions were scored on a 1-5 basis, and where an organisation did not feel it was relevant to a question then no answer was given. The findings reflect answers that returned a response of 4 or 5 (important or very important).

They are presented in no particular order.

2.2. Cyber security findings

Smart metering has many security features built into it due to the sensitivity of a 3rd party gaining access to large loads, and it is likely the smart grid will be switching equally large loads and is equally sensitive.

The key priorities for Cyber Security from the questionnaire are tabulated in Table 1:

ID	Policy finding
PF1	A security assurance scheme must be put in place for systems and system actors (eg suppliers and chargepoint manufacturers and associated software)
PF2	Anomaly detection, or similar approach to mitigating risk of compromise (e.g. dual controls), must be implemented to act upon unusual and suspicious patterns of behaviour
PF3	Role based access control must be implemented on charging devices
PF4	Key recovery processes must be defined in case of catastrophic failures or breaches of the smart grid systems
PF5	Critical commands must be secure end to end
PF6	Chargepoints and service providers must have unique identifiers
PF7	Messages must be uniquely identifiable and able to protect against replay attacks
PF8	Chargers must be able to generate their own private keys
PF9	Supply affecting commands must be security checked by 3rd party before being actioned
PF10	Message audit trails must be maintained
PF11	Network time synchronisation must be available
PF12	Firmware must be centrally registered before it can be executed on a smart charger

Table 1. Cyber security policy findings.

PF2 and PF9 both refer to '3rd party checks' also known as 'protocol integrity checking' or 'dual controls'. This means that a 3rd party, independent from the service provider, must inspect the service provider's messages to ensure that they have not been malformed or interfered with in any way.

2.3. Grid Stability Findings

Grid stability and cyber security are inextricably linked because of the potential for hackers to switch large loads and cause rolling blackouts. Therefore, most of the cyber security findings in the cyber security question also relate this section.

However, in Table 3 are listed three further findings which are specifically related to grid stability (implicitly affecting cyber security):

ID	Policy finding
PF13	Smart functions must continue to operate during communications outages
PF14	Randomised offsets must be applied to commands which cause a change in load
PF15	DNOs must be able to determine the instantaneous and historical EV-related energy consumption

Table 2. Grid stability policy findings

These findings reveal the importance of being able to maintain smart services during communications outages (which could be quite frequent depending on the type of communications being used). Otherwise, such outages may cause maximum charge rates to be curtailed and consumer costs to rise, leading to consumer dissatisfaction with the EV charging system.

Under certain circumstances, randomised offsets may be used to smooth out grid power surges and should be available to use where appropriate. However, implementation of randomised offset needs to also be compatible with the need of DSRSPs to control load with potentially sub-second latency.

Also, DNOs need access to the historic and instantaneous consumption values to assist with network planning and operation.

2.4. Data privacy findings

To ensure trust in a smart grid system, consumers must have confidence in the data privacy measures that are implemented. Our questionnaire has found the following key requirements in this area, shown in Table 3:

ID	Policy finding
PF16	Consumers must be able to access their EV energy and consumption and charger data in a standardised format, without recourse to a 3rd party
PF17	Consumers must be able to opt out of daily reads of energy data
PF18	Anonymised data must be made available as a public good subject to consumer consent
PF19	Sensitive data must be protected end to end via cryptography

Table 3. Data privacy policy findings

Some of these findings are hygiene factors that should be built into every system, but the interesting finding here is to make anonymised data available for public good, probably in a standardised format to enable consumers and systems to interoperate and make like-for-like comparisons between service providers and other purposes.

2.5. Interoperability findings

Respondents noted that the key priorities for interoperability in an EV smart charging system are as follows in Table 4:

ID	Policy finding
PF20	The ability to change EV energy supplier, DSRSP and, in the event that it ceases operating, the CSMS, while retaining minimum device functionality without need for site visit
PF21	All smart EV chargers must support Time of Use tariffs[1] such that the consumer and/ or 3rd party can set charging schedules
PF22	Consumers must have access to and be able to provide their energy data to a 3rd party for analysis;
PF23	The EV must not be tied to a specific charger, but be able to charge at any residential chargepoint
PF24	Residential chargers should be able to provide charging to 3rd parties

Table 4. Interoperability policy findings

These findings indicate that interoperability is required not only to support switching between DSRSP and CSMS, but also, because of the complexity of smart tariffs, a degree of 'data format interoperability' may be required to enable systems to share smart tariffs and energy data for the

[1] It is assumed that this policy finding extends to other 'smart' tariffs such as flexible and 'type of use' tariffs.

purposes of billing, analysis and DSR. Without this data format interoperability, it may be difficult for systems to communicate, delaying or undermining the development of a secure and interoperable system. The complexity could be impossible for humans to manage directly, for example it may not be possible for consumers to input their smart tariff into a website or describe it to another human over the phone.

The ability to change energy supplier without the need for a site visit is already provided via the smart meter system.

No requirement for change of EVSE CSP was identified.

A level of integration with the smart metering system or web publication may be required to support smart tariffs, again requiring a degree of data format interoperability. More complex billing relationships may be required to allow 3rd parties to charge if costs are to be apportioned to the correct parties in the future and true interoperability of charging is to be achieved.

While examples of interoperability between web-based systems are widespread, there are fewer examples of interoperable systems which meet the grid stability and cyber security requirements of the smart meter system. One lesson from the smart meter rollout has been to not underestimate the challenge in achieving *secure* interoperability.

One obvious challenge to achieving interoperability is protocol translation. Apart from the need for every translator to implement the translation correctly, there is an associated cost and time impact for testing, certification, integration and deployment that must be replicated for each translation implementation.

2.6. Consumer protection findings

The consumer protection questions focussed mainly on electric vehicle charging but would be equally applicable to any large electrical load – e.g. home heating.

The priorities within consumer protection are tabulated in Table 5:

ID	Policy finding
PF25	A consumer should be able to override any flexibility system (except for reasons of safety e.g. overloading)
PF26	Consumers must be able easily to compare a bill from one EV energy provider with another
PF27	Prepayment options for energy must be available
PF28	The type of charger must not restrict consumer choice of tariff in the marketplace
PF29	The service must be available to every home in the country
PF30	EV charging must be simple and straightforward for all, including those with disabilities

Table 5. Consumer protection policy findings

The need to reach all homes will require a communications service or services that has wide coverage across all areas, including rural and inside buildings. Inner city areas can be hard to reach, particularly where EV chargers are located away from dwellings, for example in underground car parks in large city blocks.

Consumer override was also considered to be very important. The consumer interface to the system will be critical to ensure the adoption and effectiveness of any smart grid applications.

2.7. Policy principle conclusions

There are some interesting findings within the data, and findings that point to the final solution.

It is vitally important that a balance is found between the innovators who want to introduce new services and new ways for consumers to interact with their product, while protecting nationally important assets in the electricity grids.

In particular, the interoperability and security sections provide some insight into potential solution options. Some of the policy findings point to a need to implement a central systems management capability for specific functions.

For an end-to-end security system to work, a dedicated security framework should be implemented, and NCSC should and presumably will play a major role in how that framework is specified.

3. Use case analysis

The purpose of this analysis was to list the use cases that are likely to be required in the EV charging system and identify those which may need special consideration to meet the policy principles identified in section 1.5.

Several EV charging-related protocols were considered for inclusion in the analysis:

- OCPP v2.0.1
- ISO 15118-1:2017
- DUIS v1.0 (Note that v4.0 is now available which includes auxiliary proportional control capability, similar to auxiliary load control for this purpose)
- PAS 1878
- OpenADR
- EEBus

Of these, only OCPP v2.0.1 was taken forward in the analysis. The other protocols were thought to be insufficiently relevant to the policy or architectural implications for EV charging in the short term to warrant inclusion. In particular:

- ISO 15118-1:2017: As this is a front-end protocol between the EVSE and the EV, it is not thought to play a major role in the overall system-wide cyber security, grid stability or interoperability of the total system;
- DUIS v1.0: This is the smart meter back-end communications protocol and was found to represent a low impact for most of the policy findings, therefore detailed analysis was not thought to be useful;
- PAS 1878: BEIS has indicated that PAS 1878 is unlikely to be considered for inclusion in the forthcoming 2021 regulations. That said, it remains a longer-term option and may be worth considering for future work;
- OpenADR: The generic nature of the protocol means that an additional specification within the OpenADR framework would be needed to achieve the specific functionality required. Currently there are no proposals for that specification which would need to be defined down to the individual command and data item level.
- EEBus: The generic nature of the protocol means that an additional specification within the OpenADR framework would be needed to achieve the specific functionality required. Currently there are no proposals for that specification which would need to be defined down to the individual command and data item level.

OCPP v2.0.1 was chosen over the more widespread v1.6 due to the superior security provisions of the later version.

While not considered here due to its immaturity, ISO 63110 is a potential successor to OCPP and should be considered in future analyses. It may be possible to consider ISO 63110 as a successor to OCPP with the additional benefit of being internationally standardised.

3.1. Detailed OCPP use case analysis

Initially, a detailed analysis of the OCPP v2.0.1 use cases was performed to establish the general risk and impact levels associated with each low-level use case within the protocol definition. This analysis was used as a guide to the service function RAG ratings provided in section 3.2. The results of the detailed use case analysis can be found in Appendix A.

3.2. Service functions

Following the analysis of OCPP use cases, the service functions were defined and assessed. These are services that the consumer may wish to procure from the market in relation to their EV charging needs. The service functions were mapped onto OCPP protocol use case categories that would be relevant for implementation, compared with the detailed use case analysis described in section 3.1 and assessed at a high level for cyber security risk and interoperability impact according to a subjective red/amber/green rating scheme. The service functions and RAG ratings are tabulated in Table 6. This high-level assessment is used as a guide and a filter for the subsequent detailed options analysis in sections 3.3 and 3.4, meaning that service functions classified as high-risk are taken forward for option analysis. Medium and low risk service functions are not considered further at this stage.

ID	Service function (things consumers want)	OCPP Use Cases categories	Service provider(s)	Risk to grid stability / cyber security	Grid stability / cyber security note	Interoperability Impact	Interoperability note
SF1	Installation and commissioning of EVSE	A,B, C, D, K, M	EVSE Installer, EVSE CSMS	High	Multiple sources of risk, particularly in the commissioning process	Interoperability N/A	Cannot have a change of installing CPO
SF2	Supply of EV energy to residential property		Energy supplier	Low	Risks already mitigated through existing controls	Currently interoperable	Existing provision of energy supply license. Interoperable through smart metering.
SF3	Provision of EVSE smart tariff		Energy supplier	High / Low	If provided through the smart meter system, then risk is low. Otherwise potentially high	Currently interoperable	Existing energy supplier tariffs. Interoperable through smart metering.
SF4	Locally operated charging	E, I	N/A	Low	No remote connection, so risk is low	Interoperability N/A	Assumes local load balancing is in place which means 'connect and notify' applies rather than 'Apply to connect to DNO'. Charging schedule may be programmed locally.
SF5	Remote provision of instantaneous and recent (since last change of CSMS / DSRSP) charging consumption data and metadata to consumer	E, I, J	Energy supplier / CSMS / DSRSP	Medium	While privacy of the data is a concern, there are no grid stability risks, hence medium overall	Interoperability N/A.	N/A because this SF only applies since last CoSP
SF6	Provision of historical EV consumption data to consumer	J	EVSE / Energy Supplier / DCC Other User / Smart meter / EV	Medium	While privacy of the data is a concern, there are no grid stability risks, hence medium overall	Interoperability available but would need to be implemented	Interoperable through smart meter. Assumes a dedicated smart meter element measures the EV-specific consumption. If not the case then interoperability risk could be 'High'.
SF7	Remotely operated non-smart charging	F, I	Energy supplier / DSRSP / CSMS	High	Multiple grid stability risks associated with remote load control	Interoperability possibly required, but not currently available.	Assumes local load balancing is in place which means 'connect and notify DNO' applies rather than 'apply to connect to DNO'. EVSE may be configured, monitored and controlled through smart phone app including charging schedule.
SF8	Smart charging using DSR / V2G	F, G, I, J, K, M	DSRSP	High	Multiple grid stability risks associated with remote load control	Interoperability required, but not currently available.	This function should survive change of DSRSP in order to avoid lock-in and consumer dissatisfaction

SF9	'Family and friends' charging through authorisation and credential management	A, C, D, M	CSMS	Low	Some minor risk of electricity theft from individual premises	Interoperability possibly required, but not currently available.	This relates to the ability for a residential EVSE owner to give permission for a third party to use the EVSE. This does not extend to commercial arrangements (i.e. cross charging for the energy.) If a residential consumer wishes to rent their charge point out commercially then this should be classed as public charging which is out of scope of this document.
SF10	Change of EVSE configuration	A, B, C, D, K, M, N	CSMS	High	Multiple security risks including those related to grid stability	Interoperability required, but not currently available.	Charge points may need to be reconfigured through-life as a result of changes in property occupancy, vehicles, other loads in the property, changes to security credentials etc.
SF11	Maintenance of EVSE (including FW update)	L, N	EVSE Manufacturer, CSMS	High	Multiple security risks including those related to grid stability	Interoperability possibly required, but not currently available.	Although manufacturers will supply the firmware, and may be permitted to download it to the EVSE, a CSMS will probably be required to activate it.
SF12	Change of service provider		Energy supplier, CSMS, DSRSP	High	Multiple security risks including those related to grid stability (not from energy supplier)	Interoperability required, but not currently available.	Already available in respect of energy suppliers. However this function should also survive change of DSRSP in order to avoid lock-in and consumer dissatisfaction. May also need to be a means of transferring the CSMS and EVSE CSP service in the case for example that the EVSE CSP or CSMS ceases to operate.
SF13	Warranty claim		EVSE Retailer	Low		Interoperability N/A	Cannot have a change of installing CPO / reseller

Table 6. Service function definitions and high level RAG analysis.

For reference the meaning of the OCPP v2.0.1 use case categories is given in Table 7 below.

OCPP UC Category ID	Use Case Category	Category summary
A	Security	Updating passwords, certificates and profiles and security alerts
B	Provisioning	Booting, configuring, reporting and reset
C	Authorisation	Various means to ensure the user is authorised to charge
D	Local Authorisation List Management	For synchronising local authorisation lists to the CSMS
E	Transactions	Locally starting, stopping and suspending charging sessions plus reporting the transaction data
F	Remote control	Remotely starting and stopping charging sessions and unlocking the connector
G	Availability	Reporting EVSE availability data and time sync
H	Reservation	Used by CSMS to reserve EVSE
I	Tariff and cost	Show tariff and cost information on the EVSE display
J	Meter values	Sending metering information to CSMS
K	Smart charging	Various local and remote means to implement load management to ensure safe operation, protect the domestic supply and protect the grid
L	Firmware management	For updating the device firmware
M	ISO15118 Certificate management	For enabling ISO15118 features to be supported
N	Diagnostics	For configuring, retrieving and erasing diagnostic data and alerts.
O	Display message	For specifying and displaying messages on the EVSE display
P	Data transfer	For custom proprietary communications between CSMS and charge point. Not part of OCPP standard

Table 7. OCPP v2.0.1 use case category definitions

3.3. Cyber security, grid stability and data privacy risks

Each of the service functions from Table 6 that represent high risk to grid stability, cyber security or data privacy are elaborated below and, where relevant policy findings are found to have a bearing on the requirements, some potential implementation options are proposed based on the three high-level architecture options of:

1) the existing point to point architecture
2) the smart meter system
3) a third independent or hybrid option.

Note that these three options were chosen as the basis for the analysis because, in the case of 1) and 2) there are real-world examples on which to build the analysis and in the case of 3) because it was considered that combining the best features of 1) and 2) in a hybrid approach was likely to yield good results.

From a cyber security, grid stability and data privacy point of view, high risk service functions include (from Table 6):

- SF1 Installation and commissioning of EVSE

- SF3 Provision of EVSE smart tariff
- SF7 Remotely operated non-smart charging
- SF8 Smart charging using DSR / V2G
- SF10 Change of EVSE configuration
- SF11 Maintenance of EVSE (including FW update)
- SF12 Change of service provider

3.3.1. SF1 Installation and commissioning of EVSE

Apart from the physical installation of the hardware (not in scope of this document), this service function involves the initial communications network setup, configuration and bringing into service of the EVSE by the EVSE Installer or CSMS. Commissioning functions which are typically performed during the commissioning process can include:

- Service discovery
- Pre-notification
- Authorisation
- Network join
- Trust establishment
- Synchronise clock
- Configure EVSE

Each of these commissioning functions are assessed below to establish whether any relevant policy findings apply to the functions and if so, what the options might be to address those policy findings.

3.3.1.1. Service Discovery

The service provider establishes the status of the devices and communications networks to be employed during the commissioning process.

Relevant cyber security, grid protection and data privacy policy findings: None

Implementation options: No applicable policy findings therefore no implementation options identified.

3.3.1.2. Pre-notification

The devices to be commissioned are registered with a central register.

Relevant cyber security, grid protection and data privacy policy findings:

PF6: Chargepoints and service providers must have unique identifiers

PF12: Firmware must be centrally registered before it can be executed on a smart charger

Implementation options:

1) P2P option: OCPP could be upgraded with a central register specifically for GB. This may or may not be acceptable to the Open Charge Alliance (OCA) who maintains the OCPP standard.

2) Smart meter option: DCC could be used as a central register for devices and firmware with minimal modification.
3) Third option: An independent central register could be developed specifically for Great Britain's EV charger system.

3.3.1.3. Authorisation

The devices to be commissioned are validated by a central register.

Relevant cyber security, grid protection and data privacy policy findings:

PF6: Chargepoints and service providers must have unique identifiers

PF12: Firmware must be centrally registered before it can be executed on a smart charger

Implementation options:

1) P2P option: OCPP could be upgraded with a central register specifically for GB
2) Smart meter option: DCC could be used as a central register
3) Third option: An independent central register could be developed specifically for Great Britain's EV charger system.

3.3.1.4. Network join

The devices to be commissioned connect to the network.

Relevant cyber security, grid protection and data privacy policy findings: No cyber security, grid protection and data privacy policy findings apply. However attention is drawn to PF29 'The service must be available to every home in the country.'

Implementation options: No relevant policy findings identified

3.3.1.5. Trust establishment

Trust is established between the charge station and the service provider through the exchange of security credentials using public key cryptography.

Relevant cyber security, grid protection and data privacy policy findings:

PF3: Role based access control must be implemented on charging devices

PF5: Critical commands must be secure end to end

PF6: Chargepoints and service providers must have unique identifiers

PF7: Messages must be uniquely identifiable and able to protect against replay attacks

PF8: Chargers must be able to generate their own private keys

PF9: Supply affecting commands must be security checked by 3rd party before being actioned

Implementation options: These are described below for each of the relevant policy findings:

3.3.1.5.1. Policy finding PF3. Role based access control (RBAC) must be implemented on charging devices.

Relevant service providers include EVSE Installer, EVSE Maintainer, CSMS, DSRSP. RBAC generally requires a central authority to provide role or organisational permissions to users which define the services they are permitted to provide. The firmware on the endpoint, in this case EVSE, may also be specified and potentially assured to enable service providers to only access functions for which their role is permitted.

1) P2P Option. Upgrading OCPP to support RBAC could be considered, although it would require significant work to upgrade the protocols and general agreement on the definitions of the service providers and the services that they would be permitted to deploy.
2) Smart meter option: The DCC implements RBAC for the smart meter system as applied to DUIS/GBCS service requests and responses. Relevant (as a minimum those considered 'critical') OCPP commands could be implemented as service requests or wrapped inside GBCS for delivery under the RBAC controls. Because the framework for RBAC already exists in DUIS/GBCS, it ought to be straightforward to define roles and critical SRs and add them to those specifications.
3) Third option: An alternative implementation option could involve the establishment of a separate central supervisor to manage the provision of permissions to the various service providers. P2P service providers could check with the new authority when wishing to send a message that they were permitted to do so, either for every message or for a sample of messages, to check that they were conforming to specific rules including RBAC permissions. Significant work to develop the protocols and message structures would be required to implement this option.

3.3.1.5.2. Policy finding PF5. Critical commands must be secure end to end.

Relevant service providers include EVSE Installer, EVSE Maintainer, CSMS, DSRSP. Public key cryptography is generally used to ensure the integrity and/or confidentiality of messages. The level of trust afforded to the root certification authority (RCA) is of primary interest.

1) P2P option: OCPP encryption is based on TLS and public key cryptography, however it relies on access control at the server to ensure that security mechanisms cannot be bypassed which could be considered a potential vulnerability. While the use of commercially available certification authority services is common for OCPP systems, the RCA for OCPP is not specified, therefore it may be possible to accredit commercial RCA providers and require that EV service providers only use those accredited RCA providers. The OCPP topology can support third party service providers (for example a DSRSP). If OCPP security were to be employed, the highest level security profile (level 3) should be mandated.
2) Smart meter option: In the smart meter system the RCA was chosen specifically according to a wide range of requirements and implements a much greater degree of sophistication and capability than OCPP, particularly around the specification of the RCA, the establishment of separate PKIs for devices, DCC and infrastructure. However, some changes would be required to GBCS e.g. user roles and device definitions.
3) Third option: A new RCA could be established with GB-specific requirements and managed under a new EV infrastructure security body. Service providers could be mandated to connect to this new facility using specified procedures for receiving or

validating key material, providing the non-repudiation required and enforcing recovery and revocation procedures in the event of a breach. Associated with the RCA could be a central supervisor function which provides key management services when a change of service provider is required (see section 3.3.7.) Note that any impact on existing certification services that manufacturers may have put in place to secure proprietary systems may need to be considered.

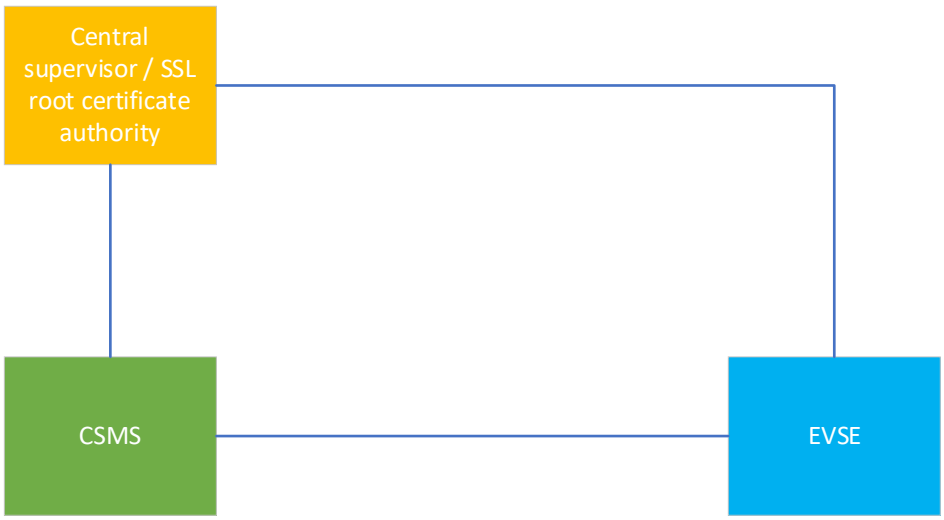


Figure 3. Central supervisor option.

3.3.1.5.3. Policy finding PF6. Chargepoints and service providers must have unique identifiers

1) P2P option: OCPP requires that a unique serial number is assigned to the charging station. However, there is no indication of how the uniqueness of the serial numbers is to be achieved.
2) Smart meter option: The smart meter system uses the MAC addressing system to uniquely identify each asset on the network and these are verified as being unique through a process of certificate validation over the smart metering key infrastructure (SMKI).
3) Third option: A new central register, in line with that proposed in section 3.3.1.2 could be established to meet the specific requirements of the EV charging system.

3.3.1.5.4. Policy finding PF7. Messages must be uniquely identifiable and able to protect against replay attacks.

1) P2P option: OCPP does not appear to have any facility to protect against this. It might be possible to extend OCPP with a GB-specific facility to apply monotonically increasing message counters to each message. Corresponding counter checks would need to be added to the EVSE firmware along with a system of testing to ensure the function worked correctly.
2) Smart meter option: The smart meter system uses a system of message counters in the originating message and also in the meter firmware to protect against replay. OCPP payloads wrapped in GBCS headers would benefit from this anti-replay system.

3) None identified.

3.3.1.5.5. Policy finding PF8. Chargers must be able to generate their own private keys.

1) P2P option: OCPP requires that the charge station shall be able to generate its own public/private key pairs. However, to benefit from this requires security profile 3 (TLS with client side certificates) to be employed.

2) Smart meter option: SMETS requires that smart meters are able to generate their own private keys and that the device hardware can support the relevant key generation requirements e.g. entropy level.

3) Third option: Charge points could be required to meet certain requirements in addition to OCPP which specified how the keys were to be generated in the device, either during manufacture or installation / commissioning. A security companion specification to OCPP could mandate some of the optional aspects of OCPP (e.g. security profile 3) and elaborate some specific procedures that were required to enhance the OCPP provisions.

3.3.1.5.6. Policy finding PF9. Supply-affecting commands must be security checked by 3rd party before being actioned

1) P2P option: This policy finding requires that supply-affecting commands are inspected and verified as legitimate by a party independent of the originating party before the command can be sent to the recipient. OCPP doesn't provide for this capability, so the P2P solution as it stands could be augmented with a dual control solution, whereby following its creation, the critical command is sent to a third party validation service, checked, signed if found to be valid and then returned to the originator for sending to the recipient. A solution similar to the DCC SMETS1 Enrolment and Adoption Dual Control Operations (DCO) might be appropriate, but perhaps developed independently for the specific purposes of the EV charging network to meet the requirements for latency, security assurance etc. The serial nature of the DCO approach implies there could be an added latency associated with a DCO that may make this option impractical for certain fast response DSR functions.

2) Smart meter option: The DCC uses a combination of a protocol checking function called 'parse and correlate' alongside integrity checking using digital signatures to ensure that every critical (supply-affecting) command is verified as being legitimate before it is sent to the recipient. There is a latency associated with this function that may mean this approach is impractical for certain fast response DSR functions.

3) Rather than apply dual controls at the service provider end of the network, it may be simpler to apply a supervisory function at the EVSE end of the network. This could take the form of a secure device, perhaps connected via the smart meter network for security, similar to the concept of the standalone auxiliary proportional controller (SAPC) which would need to provide its approval to the EVSE before any change in load could take place. If frequency measurement were included at the endpoint then potentially the supervision of fast frequency control could be made to be autonomous, again through a securely connected supervisor device.

3.3.1.6. Synchronise clock

Commissioning function: Synchronise clock

Description: The device to be commissioned synchronises its clock with the service provider.

Relevant cyber security, grid protection and data privacy policy findings:

PF11: Network time synchronisation must be available

Implementation options:

1) P2P option: The OCPP heartbeat use case (G02) can be used to synchronise the charging station clock with that of the CSMS. This function is optional within the OCPP protocol but could potentially be made mandatory for a GB-specific implementation of OCPP. Some means of detecting bad time in the service provider system may also be required to prevent cyber attacks.
2) Smart meter option: The smart meter system implements a secure clock synchronisation process via the communications hub.
3) Third option: Alternatively various third party time protocols exist e.g. network time protocol (NTP), mobile network. OCPP optionally supports a number of these. A trust relationship with the time source would be required to ensure the integrity of the time being distributed to the charge stations.

3.3.1.7. Configure EVSE

See section 3.3.5.

3.3.2. SF3 Provision of EVSE smart tariff

This service function includes the delivery of a smart tariff from the energy supplier to other actors including CSMS, EVSE and potentially DSRSP. This is a high risk function because the intention is to use it to modify load scheduling in order to achieve peak shifting. The DSRSP may or may not require the smart tariff in order to deliver their service, but it is included here on the assumption that it is possible if the consumer permits it.

Relevant cyber security, grid protection and data privacy policy findings:

PF2: Anomaly detection, or similar approach to mitigating risk of compromise (e.g. dual controls), must be implemented to act upon unusual and suspicious patterns of behaviour

PF3: Role based access control must be implemented on charging devices

PF5: Critical commands must be secure end to end

PF7: Messages must be uniquely identifiable and able to protect against replay attacks

PF9: Supply affecting commands must be security checked by 3rd party before being actioned

PF10: Message audit trails must be maintained

PF11: Network time synchronisation must be available

PF13: Smart functions must continue to operate during communications outages

PF14: Randomised offsets must be applied to commands which cause a change in load

PF19: Sensitive data must be protected via end to end via cryptography

PF21: All smart EV chargers must support Time of Use tariffs

Implementation options:

Several potential routes can be taken to transfer the smart tariff from the energy supplier into the target systems. These are summarised in the matrix of Table 8 along with a description of how the option could be achieved securely.

FROM→ TO ↓	**Energy Supplier**	**DCC Other User**	**Smart meter**
CSMS	A direct P2P web services connection may require specific measures to secure each individual link between each energy supplier and each CSMS. The measures required may, depending on security assessments, include many of the protections demanded by the relevant policy findings and each may require a degree of independent security assurance. A new specification would be required to ensure the same standards of security and privacy were achieved for each bilateral connection.	If the smart tariff is to be derived directly from the smart meter system, this could be achieved via the DCC Other User interface. This would require each CSMS to either complete DCC User Entry Process Testing and thereby gain access to the DCC OU interface directly, or alternatively, several third-party DCC adaptor services are now commercially available and could be used to provide access. The CSMS would be required to undergo periodic privacy assessments under the existing framework to ensure conformance to security protocols.	The tariff residing on the smart meter in the property could theoretically be accessed via a consumer access device (CAD) if available. This may require a commercial arrangement with the CAD provider to enable the CAD tariff data to be transferred to the CSMS. However, in practice CAD connectivity is not likely to be universally available, making this option unlikely to be practical.
EVSE	N/A	N/A	If a Zigbee Type 2 logical device function were embedded within the EVSE, then the smart tariff could be transferred directly to the EVSE over the Zigbee HAN using established secure protocols. However, this would add a degree of cost to the EVSE and may not be possible in all properties due to propagation limitations (although AltHAN extenders could resolve for an extra cost.)
DSRSP	In the event that DSRSPs use the smart tariff as part of the optimisation process for the EVSE, then the smart tariff can be	If the smart tariff is to be derived directly from the smart meter system, this could be achieved via the DCC Other User interface. This would	The tariff residing on the smart meter in the property could theoretically be accessed via a consumer access device (CAD) if

	provided via a direct P2P web connection between the DSRSPs and energy suppliers. This may require specific measures to secure each individual link between each energy supplier and each DSRSP. The measures required may include many of the protections demanded by the relevant policy findings and each may require a degree of independent security assurance. A new specification would be required to ensure the same standards of security and privacy were achieved for each bilateral connection.	require each DSRSP to either complete DCC User Entry Process Testing and thereby gain access to the DCC OU interface directly, or alternatively, several third-party DCC adaptor services are now commercially available and could be used to provide access. The DSRSP would be required to undergo periodic privacy assessments under the existing framework to ensure conformance to security protocols.	available. This may require a commercial arrangement with the CAD provider to enable the CAD tariff data to be transferred to the CSMS. However, in practice CAD connectivity is not likely to be universally available, making this option unlikely to be practical.

Table 8. Smart tariff options.

Preferred options are:

From DCC Other User -> CSMS

From DCC Other User -> DSRSP

These two options represent existing secure and private mechanisms for transferring the smart tariffs, each meeting most of the relevant policy findings without requiring new specifications or security assurance schemes. However they would require CSMS and DSRSP to undergo DCC user entry process testing or otherwise contract the services of an approved 3rd party. Security assurance of the connection between CSMS/DSRSP and 3rd party is required as part of the 3rd party DCC user status. Other options making use of the Zigbee HAN to communicate securely may also be considered if individual service and asset providers wish to use that route.

3.3.3. SF7 Remotely operated non-smart charging

This service function involves consumer actions of starting, stopping and monitoring of EV charging remotely, probably via a smart phone app. Remote operation functions that would typically be performed under this service function include:

- Remote start / stop transaction
- View charging progress

Each of these remote operation functions is assessed below to establish whether any policy findings apply to the functions and if so, what the options might be to address those policy findings.

3.3.3.1. Remote start / stop transaction

The car has previously been physically connected to the EVSE and is not charging at the time the consumer wants to charge (e.g. it is outside the scheduled charge period or it has been previously

stopped remotely by the consumer.) The consumer uses a smart phone app to command the EVSE to toggle its charging state from off to on or vice versa.

Relevant cyber security, grid protection and data privacy policy findings:

PF2: Anomaly detection, or similar approach to mitigating risk of compromise (e.g. dual controls), must be implemented to act upon unusual and suspicious patterns of behaviour

PF3: Role based access control must be implemented on charging devices

PF5: Critical commands must be secure end to end

PF7: Messages must be uniquely identifiable and able to protect against replay attacks

PF9: Supply affecting commands must be security checked by 3rd party before being actioned

PF10: Message audit trails must be maintained

PF25: A consumer should be able to override any flexibility system (except for reasons of safety e.g. overloading)

Implementation options:

1) P2P option: In this option (Figure 4), the consumer uses a smart phone app to send a Start/Stop Charging command directly to the CSMS using a proprietary or non-proprietary protocol as appropriate. This command is converted into OCPP at the CSMS and transmitted to the EVSE for implementation. PF2 anomaly detection and PF9 dual control 3rd party checks may necessitate specific requirements within the smart phone app or CSMS. PF3 and PF5 may not be possible in this scenario. Specific measures may be required at the CSMS to implement PF7, PF10 and PF14.

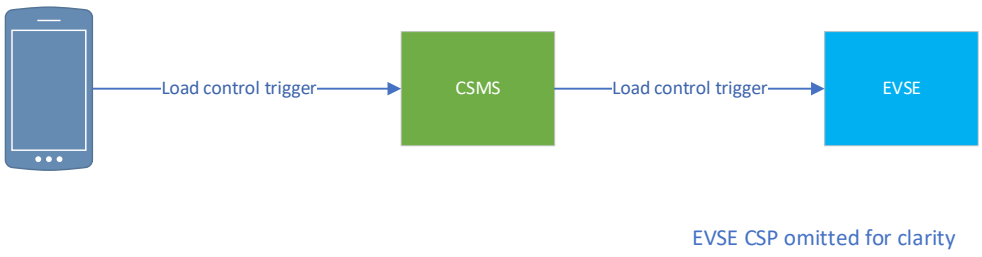
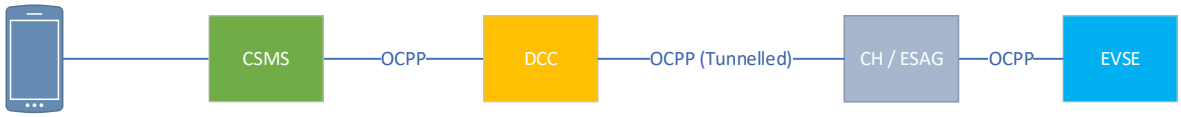


Figure 4. P2P remote start/stop

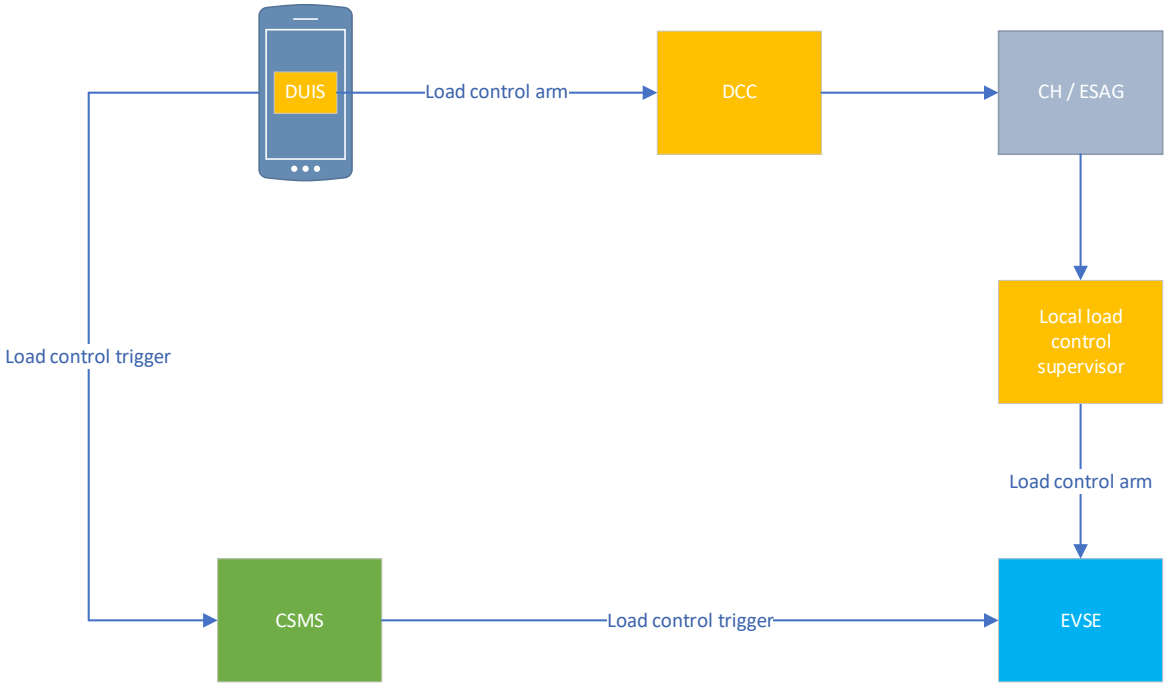
2) Smart meter option: In this scenario, the consumer uses the smart phone app to send a command in any appropriate protocol to the CSMS to start or stop charging. This is then be transformed into OCPP format by the CSMS which would wrap the OCPP command inside DUIS for delivery to the DCC. The CSMS, acting in its own, new DCC user role, may require a DCC adaptor to interface to the DCC. Security functions such as anomaly detection and protocol integrity checking are provided by the DCC. The EVSE would need to be connected to the smart meter HAN via Zigbee and requires a GBCS stack to unpack the OCPP payload for implementation. This option would also require a security certificate to be installed on the consumer device. The benefit of this approach is the ability to fulfil most of the policy findings, except for PF5 'Critical commands must be secure end-to-end', because of the need for protocol translation at the CSMS.



EVSE CSP omitted for clarity

Figure 5. Smart meter remote start / stop

3) Third option: A combination of option 1 and local arming over the smart meter system could potentially allow all the policy findings including PF5 'Critical commands must be secure end-to-end' to be achieved. Approved code from an approved vendor would be integrated into the smart phone app which would allow a local arming command to be sent to the EVSE via the DCC and ESAG. The end-to-end secure arming function would authorise the trigger command to be implemented by the EVSE. The latency of the arm command over the DCC would need to be acceptable for the consumer experience and it may need to be time-limited in order to remain secure. Advantages of this approach are that smart meter security measures are enforced upon the interoperable LLCS endpoint. Logically it is similar to a SAPC. However timing thresholds would need to be designed carefully to avoid unacceptable latency between sending the start/stop command and its implementation. One possible variant of this solution might be to integrate the DCC code into the CSMS, although this would require a relaxation of the policy finding regarding end-to-end security.



EVSE CSP omitted for clarity

Figure 6. Hybrid remote start / stop with local load control supervision of load control trigger.

3.3.3.2. View charging progress

The consumer views the charging progress directly on their smart phone app.

Relevant cyber security, grid protection and data privacy policy findings:

PF19: Sensitive data must be protected via end to end via cryptography

Implementation options:

1) P2P option: Data deriving from the chargepoint metering element is sent directly from the CSMS cloud to the consumer's smart phone. OCPP has provisions for encryption of data. Messages between the CSMS and the charge point and the provisions of section 3.3.1.5 should be taken into account, particularly the need to mandate the highest level OCPP security profile. For the connection between the service provider's cloud and the consumer's smart phone, it may be sufficient to implement TLS to ensure the privacy of the data.
2) Smart meter option: If a physical smart meter were installed alongside the EVSE, then EVSE specific energy consumption could be provided directly and securely to the consumer via the smart meter system. Apps already exist which can provide this data as a service directly from the DCC Other User interface, allowing integration with the CSMS user interface for a more integrated consumer experience. For example see www.greenely.se. It may be helpful to update the SMETS2 specification to allow a second metering element to be physically separated from the boundary meter, as this would provide more flexibility in the installation approach for this scenario.
3) Third option: As alluded to in option 2 above, if the EV chargepoint were metered directly through SMETS then the consumption data could be passed securely to the CSMS and/or DSRSP via the other user interface for integration into the CSMS / DSRSP consumer apps.

3.3.4. SF8 Smart charging using DSR / V2G

This service function involves DSRSP configuration, monitoring and control of the EVSE to deliver a range of demand side response services to aggregators, DNOs/DSOs and National Grid. In circumstances where PAS1878 compliant infrastructure is in place, then a Consumer Energy Manager (CEM) may also be involved, although this is not considered here. The smart charging functions required include:

- Read EVSE DSR Data
- Configure EVSE for DSR
- Start / stop charging with charging profile (routine mode)
- Start / stop charging on demand (response mode)

Each of these smart charging functions is assessed below to establish whether any cyber security, grid stability or data privacy policy findings apply to the functions and if so what the options might be to address those policy findings.

3.3.4.1. Read EVSE DSR Data

A wide range of device parameters are sent from the EVSE to the DSRSP to enable the DSRSP to determine the DSR capabilities of the EVSE and potentially EV.

Relevant cyber security, grid protection and data privacy policy findings:

PF3: Role based access control must be implemented on charging devices

PF19: Sensitive data must be protected end to end via cryptography

Implementation options:

1) P2P option: PF3 requires role based access control (RBAC) to be implemented, however OCPP does not currently support it. Therefore to enable PF3 would require either OCPP to be updated to include RBAC (which would require wide industry agreement and potentially a GB-specific variant of OCPP) or alternatively OCPP native messages could be wrapped in message headers which implemented the RBAC functionality. See also 3.3.1.5.1.

   PF19 (end-to-end encryption) is already implemented in OCPP, however only for the CSMS to EVSE connection. To enable end-to-end encryption to the DSRSP would require an update to OCPP or extension through the OCPP data transfer mechanism (use Case Category P in Table 7).

2) Smart meter option: RBAC is an existing feature of DUIS / GBCS and could be implemented via DCC. Relevant OCPP commands could be implemented as DUIS / GBCS service requests / responses or wrapped in DUIS/GBCS and sent through the smart meter system. The EVSE would require a Zigbee radio and GBCS stack to interpret the messages. The CSMS would need to act as a router to forward commands and data from and to the DSRSP.

3) Third option: Do not implement RBAC and allow CSMS to forward messages to the intended recipients on behalf of DSRSP. A centralised supervisory function could be used to check for anomalies, protocol integrity and security credentials of previously registered participants, enabling certificate revocation if any issues were discovered. Although this approach would not prevent suspicious messages from being delivered, it could alert service providers to the presence of a threat and, potentially, revoke certificates if certain thresholds were exceeded. This approach is shown in Figure 7 below.

   One question arising with this option is the level to which anomaly detection can be performed given that the messages may be encrypted. With end-to-end encryption in place, the central supervisor may need special access within the system to be able to inspect payloads and detect protocol anomalies. A level of analysis may also be required to determine anomaly detection threshold levels.

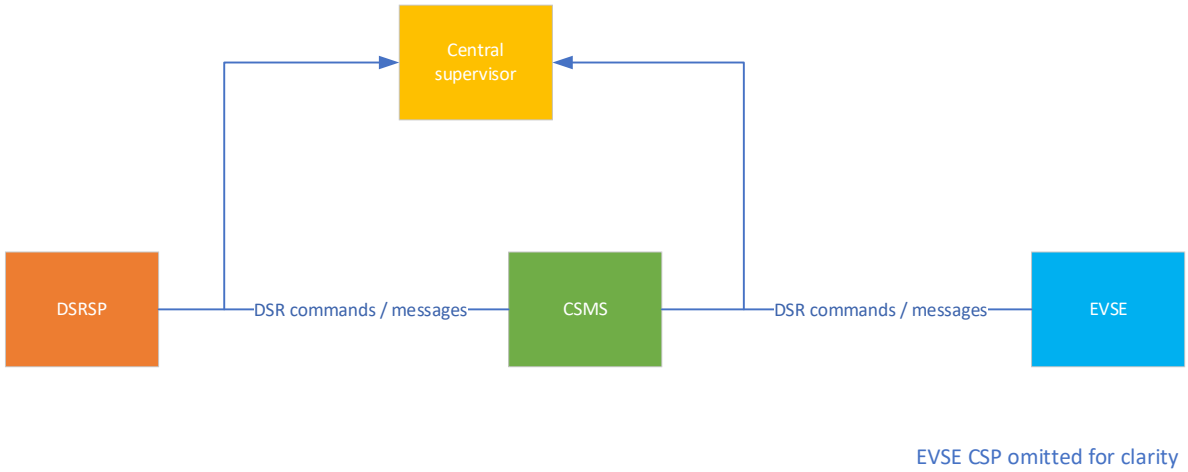


Figure 7. Central supervisor improves security of DSR messages

3.3.4.2. Configure EVSE for DSR

A wide range of device parameters are sent from the DSRSP to the EVSE to enable the DSRSP to control the DSR of the EVSE.

Relevant cyber security, grid protection and data privacy policy findings:

PF2: Anomaly detection, or similar approach to mitigating risk of compromise (e.g. dual controls), must be implemented to act upon unusual and suspicious patterns of behaviour

PF3: Role based access control must be implemented on charging devices

PF5: Critical commands must be secure end to end

PF7: Messages must be uniquely identifiable and able to protect against replay attacks

PF9: Supply affecting commands must be security checked by 3rd party before being actioned

PF10: Message audit trails must be maintained

PF19: Sensitive data must be protected end to end via cryptography

Implementation options: Many of the policy findings and architecture options from this section are the same as those for Trust Establishment and Remote Start / Stop transaction.

3.3.4.3. Start / stop charging with charging profile (routine mode)

In this scenario, the DSRSP is responsible for managing the routine mode charging schedule that is downloaded to the EVSE and controls the charging profile.

As this is effectively the same as a configuration of the EVSE, the relevant policy findings and Implementation options are the same as for Trust Establishment and Remote Start / Stop transaction. See section 3.3.1.5 and 3.3.3.1.

3.3.4.4. Start / stop charging on demand (response mode)

This smart charging function is similar to SF7, ‘Remotely operated non-smart charging’. Some differences arise due to:

- the fact that the DSRSP initiates the load control command rather than the consumer and may wish to change the load to any level between fully importing and fully exporting, including fully off;
- depending on the type of DSR service being provided, the command may need to be actioned very quickly, potentially within 1 second of it being sent. Although there are no policy findings indicating the need for this requirement, it is thought to be necessary for certain frequency response services.

Relevant cyber security, grid protection and data privacy policy findings:

PF2: Anomaly detection, or similar approach to mitigating risk of compromise (e.g. dual controls), must be implemented to act upon unusual and suspicious patterns of behaviour

PF3: Role based access control must be implemented on charging devices

PF5: Critical commands must be secure end to end

PF9: Supply affecting commands must be security checked by 3rd party before being actioned

PF25: A consumer should be able to override any flexibility system (except for reasons of safety e.g. overloading)

Implementation options:

1) P2P option: In this scenario, the DSRSP sends a command to the EVSE via the CSMS to start or stop charging. An anomaly detection system would be required either at the DSRSP or CSMS to detect unusual patterns of behaviour. To meet the requirements for 3rd party validation, the command may also be sent separately to a 3rd party dual control organisation for independent checking, signing and sending back to the DSRSP for correlation with the original DSRSP command and subsequent transmission to the EVSE, via the CSMS, for implementation. This system would need to be designed specifically to meet the latency constraints needed for this function and may require the use of approved, perhaps centrally generated and managed code to perform certain critical functions, for example anomaly detection. Depending on the protocol used by the DSRSP, protocol translation may be required between the DSRSP and CSMS which may have implications for interoperability.
2) Smart meter option: In this scenario, DSRSP sends a pre-command to the DCC using RBAC. This is then transformed into GBCS format for end-to-end delivery and returned to the DSRSP who verifies that the command is identical to the command being requested, signed, and sent to the DCC as a signed pre-command for onward transmission directly to the EVSE using RBAC. Anomaly detection is provided by the DCC. The EVSE would require a Zigbee radio and GBCS stack to extract the payload for implementation. It would also need to inform the CSMS of the transaction in order to remain synchronised with the CSMS. This approach may not offer the sub-second latency required for this function.
3) Third option: A hybrid P2P / smart meter solution could implement dual controls whereby a local supervisor device in the premise is connected via the smart meter network (similar to a SAPC in principle). This could act as an ‘arming’ control function for load control commands requiring fast response time. In order to know when to arm

the EVSE for a trigger command, this option would also need to verify independently the condition that led to the load control event, for example grid frequency drifting outside a specified range. Given the universal nature of the frequency parameter across large sections of the grid, this could be measured at the supervisor end point subject to measurement accuracy requirements. Figure 8 below shows this option in more detail.

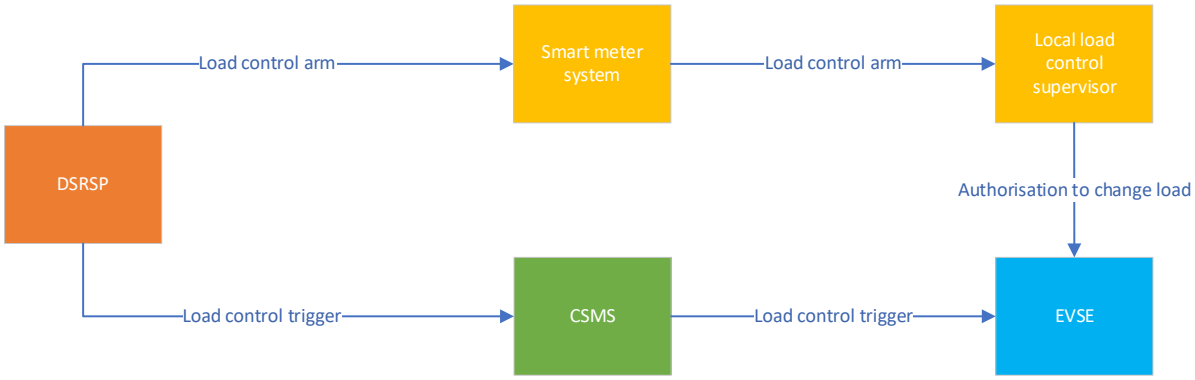


Figure 8. Local load control supervision of start / stop on demand

3.3.5. SF10 Change of EVSE configuration

A wide range of device parameters are sent to and received from the EVSE to enable the CSMS to control the EVSE.

Relevant cyber security, grid protection and data privacy policy findings:

PF2: Anomaly detection, or similar approach to mitigating risk of compromise (e.g. dual controls), must be implemented to act upon unusual and suspicious patterns of behaviour

PF3: Role based access control must be implemented on charging devices

PF5: Critical commands must be secure end to end

PF7: Messages must be uniquely identifiable and able to protect against replay attacks

PF9: Supply affecting commands must be security checked by 3rd party before being actioned

PF10: Message audit trails must be maintained

PF19: Sensitive data must be protected end to end via cryptography

Implementation options: Many of the policy findings and architecture options from this section are the same as those for Trust Establishment and Remote Start / Stop transaction. See section 3.3.1.5 and 3.3.3.1.

3.3.6. SF11 Maintenance of EVSE (including FW update)

This service function involves change of EVSE configuration (dealt with in section 3.3.5) and EVSE firmware update. A firmware update involves three main steps:

- Download of the new firmware image onto the EVSE by the EVSE maintainer;
- Integrity checks to make sure that the firmware image on the EVSE is the one that was intended to be sent by the EVSE maintainer and that it has not been corrupted or tampered with on its route to the EVSE;
- Activation of the new firmware on the EVSE, involving unpacking, installation and rebooting of the EVSE to execute the new firmware.

Relevant cyber security, grid protection and data privacy policy findings:

PF2: Anomaly detection, or similar approach to mitigating risk of compromise (e.g. dual controls), must be implemented to act upon unusual and suspicious patterns of behaviour

PF3: Role based access control must be implemented on charging devices

PF5: Critical commands must be secure end to end

PF7: Messages must be uniquely identifiable and able to protect against replay attacks

PF9: Supply affecting commands must be security checked by 3rd party before being actioned

PF10: Message audit trails must be maintained

PF11: Network time synchronisation must be available

PF12: Firmware must be centrally registered before it can be executed on a smart charger

PF19: Sensitive data must be protected end to end via cryptography

Implementation options:

1) P2P option. OCPP implements a firmware update facility for downloading the new image from an EVSE Manufacturer, although without the security level demanded by the relevant policy findings. Solutions for some of these policy findings may also be required and implemented using approaches described in previous sections (notably section 3.3.1.5, 3.3.1.6 and 3.3.3).

   However, PF12 requires a central firmware register to be maintained which has not been considered up to this point. A central firmware register could be quite straightforward to implement, either using a central register of the kind described in section 3.3.1.2 or using a separate web-based system.

2) Smart meter option. The smart meter system implements a secure firmware download, integrity checking and activation solution, including a central register called the central products list (CPL). The firmware could be downloaded to either the communications hub or the local load control supervisor in the premise for subsequent transfer to the EVSE. Activation could be by critical command provided via the local load control supervisor, similar to Figure 6.

3) Third option: It may be desirable to provide firmware image downloads from a central supervisor (Figure 9). Firmware would be provided by approved manufacturers, registered and integrity checked before being published for download. Activation of the firmware could still be applied in accordance with smart metering, using the local load control supervisor in the premise to ensure security. If sent over the open internet, strong encryption of the images should be mandated so that interception of the image by hackers cannot result in disassembly of the firmware and subsequent exploitation.

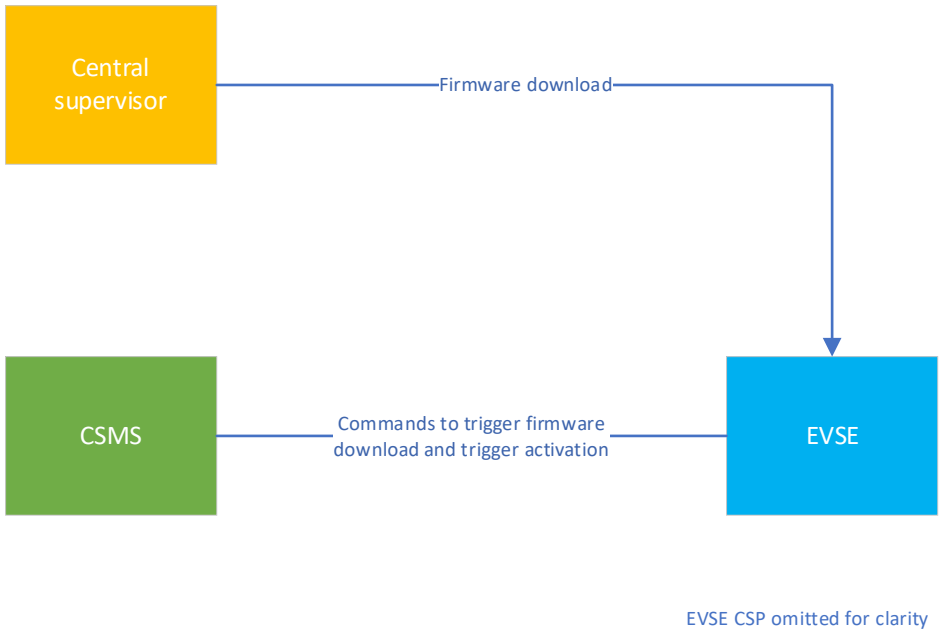


Figure 9. Firmware download via central supervisor

3.3.7. SF12 Change of service provider (CoSP)

This service function involves a change of CSMS or DSRSP, either because the consumer wishes to change their service provider for another or because the existing service provider has ceased operating.

Change of service provider consists of the following high level CoSP functions:

- Update security credentials on EVSE
- Change of EVSE configuration
- Provision of EVSE smart tariff

Secure change of service provider depends on being able to transfer security certificates without compromise. For this to happen securely may require a central supervisor function such as is described in section 3.3.1.5 and shown below in Figure 10 (noting that any impact on existing certification services that manufacturers have put in place to secure proprietary systems may need to be considered.)

Change of DSRSP is required to ensure consumers can switch DSRSP as part of a competitive market for DSR services. It may be less important to be able to switch CSMS, unless the original CSMS ceases operating, in which case a change of CSMS will be needed in order to retain the EVSE functionality.

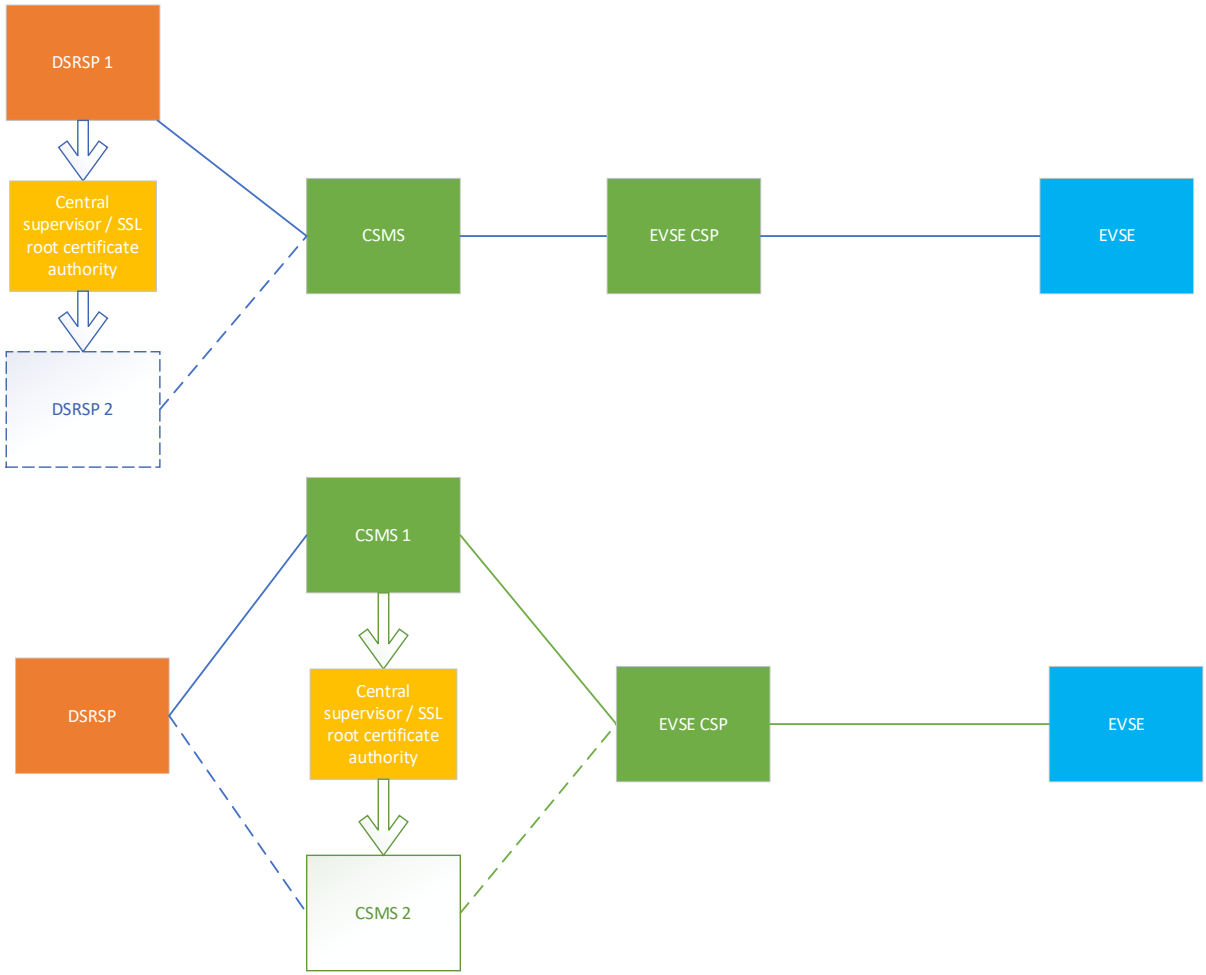


Figure 10. Secure change of service provider

Change of EVSE configuration and Update EVSE smart tariff are dealt with in sections 3.3.5 and 3.3.2.

3.4. Interoperability impacts

Each of the service functions from Table 6 that have a significant impact on interoperability and are therefore rated as “High” are elaborated below and, where relevant policy findings are found to have a bearing on the requirements, some potential interoperable implementation options are proposed based on the three architecture options of:

1) the existing point to point architecture
2) the smart meter system
3) a third independent or hybrid option.

Note that these three options were chosen as the basis for the analysis because, in the case of 1) and 2) there are real-world examples on which to build the analysis and in the case of 3) because it was considered that combining the best features of 1) and 2) in a hybrid approach was likely to yield good results.

From an interoperability point of view, high impact service functions include:

- SF8 Smart charging using DSR / V2G

- SF10 Change of EVSE configuration
- SF11 Maintenance of EVSE (including FW update)
- SF12 Change of service provider

One of the key considerations for improving the interoperability of the solution options described below has been to ensure that any translation functions are kept to a minimum, as that can be where challenges with interoperability arise in practice. One of the key lessons of the smart meter rollout has been the significant effort required to move beyond designing a secure interoperable solution and achieving secure interoperability in practice.

3.4.1. SF8 Smart charging using DSR / V2G

This service function involves DSRSP configuration, monitoring and control of the EVSE to deliver a range of demand side response services to aggregators, DNOs/DSOs and National Grid. In circumstances where PAS1878 compliant infrastructure is in place, then a Consumer Energy Manager (CEM) may also be required, located either within the DSRSP system or within the premise, although this is not discussed here[2]. The smart charging functions required include:

- Read EVSE DSR Data
- Configure EVSE for DSR
- Start / stop charging with charging profile (routine mode)
- Start / stop charging on demand (response mode)

Each of these smart charging functions is assessed below to establish whether any interoperability policy findings apply to the functions and if so, what the options might be to address those policy findings.

3.4.1.1. Read EVSE DSR Data

A wide range of device parameters are requested and retrieved from the EVSE by the DSRSP to enable the DSRSP to determine the DSR capabilities of the EVSE and potentially the EV. This includes parameters such as for example EVSE identifiers, status, power available, energy available, meter readings and local mains frequency.

Relevant interoperability policy findings:

> PF20: The ability to change EV energy supplier and other service providers without changing EV charging equipment and vice versa

Implementation options:

1) P2P Option: Within OCPP, the only party capable of reading the EVSE data is the CSMS. Therefore any retrieval of EVSE data must be conducted by the CSMS at the request of the DSRSP. To remain interoperable following change of DSRSP, this communication protocol between the DSRSP and CSMS must be standardised. OpenADR is a potential option for achieving this, but the generic nature of the protocol means that an additional specification within the OpenADR framework would be needed to achieve

[2] While PAS1878 has been developed specifically to support interoperability and is therefore a potential future option for DSR interoperability, it has not yet been developed to the protocol level and therefore it is not possible to assess it for interoperability performance at this time.

the specific functionality required. Currently there are no proposals for that specification which would need to be defined down to the individual message and data item level. This would require extensive development, testing and a certification scheme to ensure that the required functionality was achieved and that it was interoperable between DSRSPs.

Note that it is also possible to envisage a similar P2P solution between the DSRSP and the EVSE, in parallel with the connection between the CSMS and EVSE. If parallel control were employed, special methods for deconflicting the two may need to be implemented to stop them from fighting each other e.g. prioritisation, damping and hysteresis to prevent instabilities. Such methods may need to be specified and standardised in order not to jeopardise the ability for the two controllers to work properly at the same time. Furthermore, to enable correct operation of both CSMS and DSRSP, the CSMS must be able to be updated with EVSE changes caused by DSRSP and vice versa. This requires protocol translation, push alerts or other synchronising mechanism either within the EVSE or between the CSRSP and CSMS, potentially reducing the interop level. PAS1878 defines a hierarchy of control and push alerts mechanism which may be useful in this respect, although the data model and message structures for doing so are not defined.

2) Smart meter option: The RBAC facility within smart metering would allow a DSRSP to send a tunnelled OCPP command directly to the EVSE and receive a response. CoSP is also available within the smart metering system via the enduring change of supplier (ECoS) mechanism which could be extended to support change of DSRSP.

3) Third option: Another potential option to enable a P2P architecture could be to require a 'virtual' EVSE to be installed on the CSMS, shown in Figure 11.

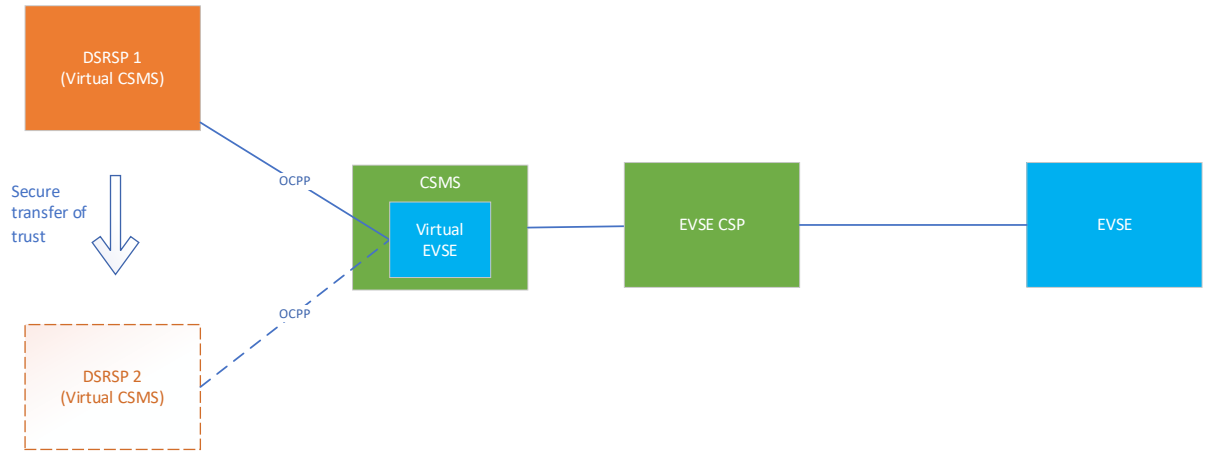


Figure 11. Virtual EVSE for DSRSP interoperability.

In this case, the DSRSP would be required to implement a virtual CSMS running an OCPP stack, although only the functionality required for DSR services would need to be implemented. The corresponding functionality would be required in a virtual EVSE, which would run within the actual CSMS. A mechanism to stimulate the CSMS into forwarding the DSRSP command and returning the response would be required within the CSMS, but this mechanism would have a low impact on the interoperability of the solution, being merely a message forwarding function. When change of DSRSP were instigated, a CoSP process would be implemented to enable security keys / certificates

to be passed from the losing DSRSP to the gaining DSRSP. How this is to be achieved in practice requires further investigation but could potentially require a central supervisor function and subsequent recommissioning of the virtual EVSE to establish trust via the TLS protocol which is the basis for confidentiality within OCPP.

Note that the need for a virtual EVSE is obviated if the DSRSP and CSMS are combined in one entity, which is likely to be the case in many circumstances.

3.4.1.2. Configure EVSE for DSR

A wide range of device parameters are sent to the EVSE by the DSRSP to enable the DSRSP to provide DSR capabilities. This includes parameters such as for example EVSE identifiers and charging profiles containing schedules and power / current limits.

Relevant interoperability policy findings:

PF20: The ability to change EV energy supplier and other service providers without changing EV charging equipment and vice versa

PF21: All smart EV chargers must support Time of Use tariffs

Implementation options: The implementation options are the same as for Read EVSE DSR Data. Please see section 3.4.1.1.

3.4.1.3. Start / stop charging with charging profile (routine mode)

In this scenario, the DSRSP is responsible for managing the routine mode charging schedule that is downloaded to the EVSE and controls the charging profile.

As this is effectively the same as a configuration of the EVSE, the relevant policy findings and implementation options are the same as for Configure EVSE for DSR. Please see section 3.4.1.2.

3.4.1.4. Start / stop charging on demand (response mode)

This smart charging function is the same as '3.3.4.4 Start / stop charging on demand (response mode)'.

Relevant interoperability policy findings: PF20

Options for implementation: The three options defined in section 3.3.4.4 are:

1) P2P option: Using a 3rd party integrity checking service which would add latency to the start / stop command. From an interoperability perspective, the implementation issues are the same as for Read EVSE DSR Data. Please see section 3.4.1.1.
2) Smart meter option: The smart meter system already implements a 3rd party integrity checking service but may not be able to meet the latency requirements. From an interoperability perspective, the implementation issues are the same as for Read EVSE DSR Data. Please see section 3.4.1.1.
3) Third option: A hybrid P2P / Smart meter solution which uses a local load control supervisor to arm the EVSE ready for a load control trigger to be actioned by the DSRSP via the CSMS. This could potentially meet the latency requirements. From an interoperability perspective, a virtual EVSE could be employed within the CSMS to standardise the load control trigger command. The load control supervisor in the

premise could be specified to use the interoperability capabilities of the smart meter system. Please see section 3.4.1.1.

3.4.2. SF10 Change of EVSE configuration

A wide range of device parameters are sent to and received from the EVSE to enable the CSMS to control the EVSE.

Relevant interoperability policy findings:

PF20: The ability to change EV energy supplier and other service providers without changing EV charging equipment and vice versa

PF21: All smart EV chargers must support Time of Use tariffs

Implementation options:

Assuming that OCPP is used as the communications protocol for this service function, then the ability to interoperate is determined mainly by the cyber security concerns described in section 3.3.1.5 and 3.3.1.7.

3.4.3. SF11 Maintenance of EVSE (including FW update)

This service function involves change of EVSE configuration (dealt with in section 3.3.5) and EVSE firmware update. A firmware update involves three main steps:

- Download of the new firmware image onto the EVSE by the EVSE maintainer;
- Integrity checks to make sure that the firmware image on the EVSE is the one that was intended to be sent by the EVSE maintainer and that it has not been corrupted or tampered with on its route to the EVSE;
- Activation of the new firmware on the EVSE, involving unpacking, installation and rebooting of the EVSE to execute the new firmware.

Relevant interoperability policy findings:

- PF20: The ability to change EV energy supplier and other service providers without changing EV charging equipment and vice versa

Implementation options:

Assuming that OCPP is used as the communications protocol for this service function, then the ability to interoperate is determined mainly by the cyber security concerns described in section 3.3.6.

3.4.4. SF12 Change of service provider

This service function involves a change of CSMS or DSRSP, either because the consumer wishes to change their service provider for another or because the existing service provider has ceased operating.

Change of service provider consists of the following high level CoSP functions:

- Update security credentials on EVSE
- Change of EVSE configuration
- Provision of EVSE smart tariff

Relevant interoperability policy findings:

- PF20: The ability to change EV energy supplier and other service providers without changing EV charging equipment and vice versa

Implementation options:

Assuming that OCPP is used as the communications protocol for this service function, then the ability to interoperate is determined mainly by the cyber security concerns described in section 3.3.7.

4. Candidate architecture

Sections 3.3 and 3.4 have proposed a variety of options for implementing smart charging in ways which meet the policy findings to varying degrees. In this section a candidate architecture is presented which attempts to meet the majority of policy findings. No formal scoring analysis has been conducted to objectively derive the optimum architecture from the various options presented. However, subjectively the candidate architecture presented here is thought to represent a reasonable recommendation for taking forwards in the discussion.

The key elements of the candidate architecture are:

- GB-specific root certificate authority meeting the requirements for smart charging PKI and change of service provider
- Central register of devices and firmware
- Request an update to OCPP to incorporate anti-replay message counters
- EVSEs to create their own private keys
- Time to be derived from the smart meter system
- 3rd party anomaly detection and protocol checking
- Smart tariffs to be derived from the smart meter system (either DCC or smart meter HAN)
- Certified DCC smart phone app code to support consumer remote override of charging status via local load control supervisor
- Supervised point to point connection between CSMS and EVSE
- Supervised point to point connection between DSRSP and CSMS
- Fast DSR control triggers to be protected using a local load control / frequency measurement arming function
- Firmware download from a secure central supervisor repository
- Interoperability between CSMSs achieved through OCPP compliance
- Interoperability between DSRSPs achieved through CSMS implementation of ‘virtual EVSE’

The candidate architecture is presented in Figure 12. This architecture is an attempt to synthesise the most promising architecture options from sections 3.3 and 3.4 together into a holistic system design. It may not meet all the policy findings completely, for example it will prove difficult to implement RBAC within a system that is based on OCPP for interoperability, due to the inherent lack of support for RBAC within OCPP. However, it meets many of the policy findings and may be a suitable candidate for consideration and further development.

The main features of the architecture are discussed below.

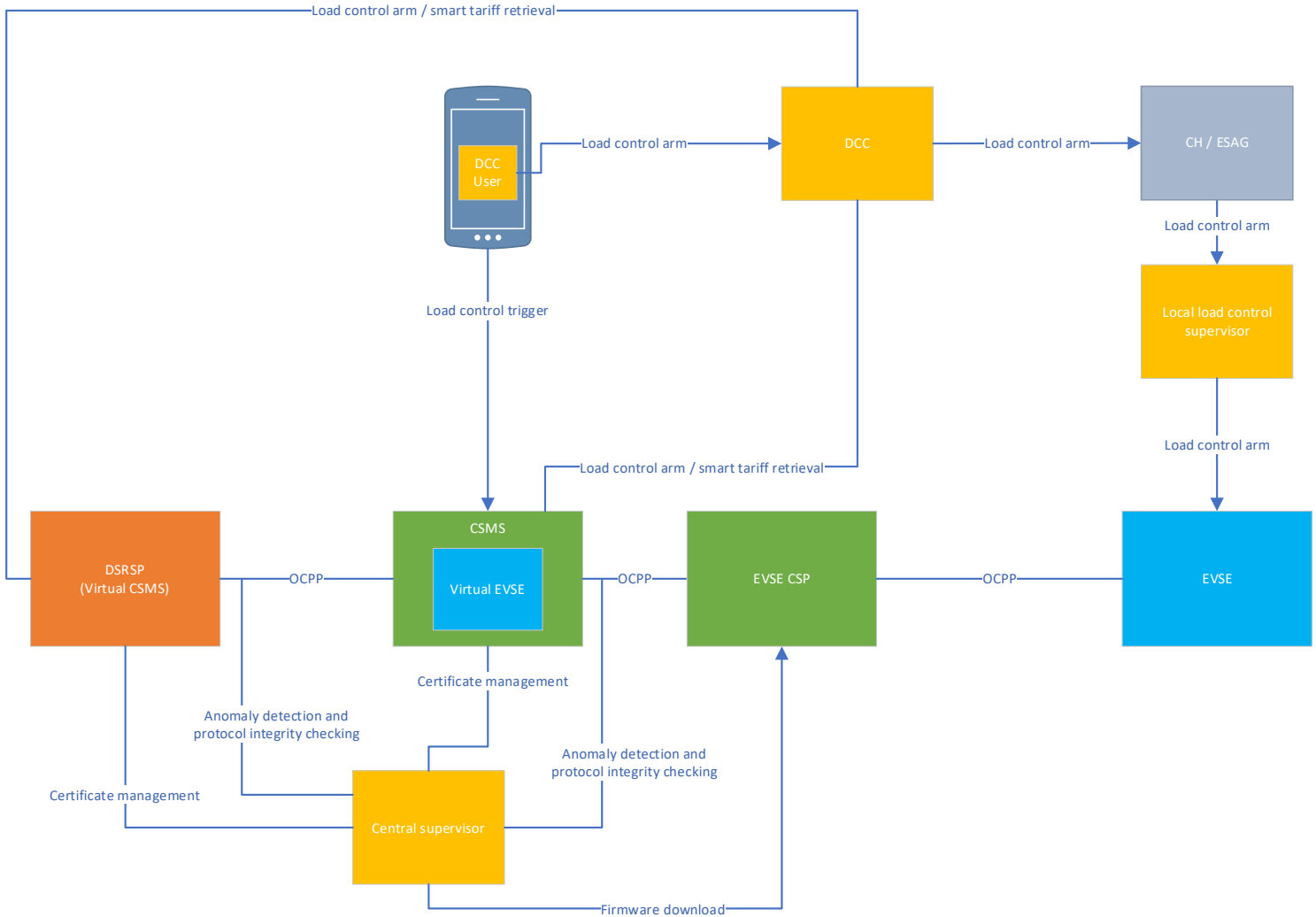


Figure 12. Smart charging candidate architecture

4.1. EVSE

The EVSE implements OCPP and communicates with the CSMS via the EVSE CSP using any suitable communications method e.g. Wifi/broadband or cellular. The local load control supervisor connects to the EVSE using any suitable communications method but possibly using a wired connection such as ethernet or serial link. A GB companion specification to OCPP should be developed and mandated to ensure that any required optional features (for example security profile) are clearly defined and mandated to ensure that the security requirements for GB can be met.

4.2. EVSE CSP

The EVSE CSP provides communications between the EVSE and the CSMS. This service can implement any suitable standardised communications service such as broadband or cellular. Interoperability of this service is achieved through the standardisation of the communications bearer. Security measures are not specified at this layer of the communications stack, relying on other layers within the system to implement the security requirements.

4.3. CSMS (Virtual ESME)

The CSMS delivers data services to the ESME (via the EVSE CSP) acting as the server for the ESMEs within its control. It receives consumer control input via the consumer's smart phone app, smart tariff information from the DCC and DSR-related messages from the DSRSP. It also communicates with the central supervisor for registration and certificate validation.

The fact that OCPP does not support RBAC means that a DSRSP may need to integrate with a CSMS to monitor and control the EVSE. In order to maintain the interoperability of the DSRSP, a standardised interface between the two is required. Given that many of the functions necessary for a DSRSP are provided within OCPP, it follows that a virtual EVSE instantiated on the CSMS will be able to create and interpret DSR-related OCPP messages to and from the DSRSP. This approach minimises the translation that might otherwise be required between the CSMS and the DSRSP and would complicate if not prevent interoperability of the DSRSP.

Note that interoperability of the CSMS is also achievable through use of the OCPP protocol which may be necessary in the event that the CSMS ceases operating and a replacement CSMS is required to maintain services to the EVSE.

4.4. DSRSP (Virtual CSMS)

The DSRSP connects to the CSMS to monitor the DSR-related parameters of the EVSE and sends DSR control triggers via the CSMS to dispatch the flexibility when required. It also receives smart tariff information if needed from the DCC and sends load control arm commands via the DCC to the local load control supervisor. It also communicates with the central supervisor for registration and certificate management.

4.5. Consumer smart phone control

A good consumer experience will be essential to market adoption of electric vehicles. This includes the ability of the consumer to control the EVSE charging status over the WAN from their smart phone. However, the security concerns with this are significant and the solution identified here may be one way to deal with this risk.

While the trigger for a load control event is always via the CSMS (which must implement its own security protocols), an additional and independent load control arming function is recommended to ensure smart meter-grade security, particularly end-to-end security, is added to the load control command. This requires that the consumer's smart phone can connect to the DCC as a DCC User to

send the load control arm command. Within the smart meter system, the process of developing and assuring the connection to the DCC is fairly involved and potentially expensive. To develop and assure this capability to run on a wide range of consumer apps could be a significant challenge but may be necessary to realise a good consumer experience while retaining the security levels required. The DCC would add a level of central control, anomaly detection, protocol integrity checking, end-to-end security and other protections which may be difficult to achieve in a point-to-point system. Many details remain to be worked out, such as how to synchronise the arm and the trigger functions, communication protocols, how the DCC User software would be specified, certified, distributed and so on. It is also possible that the direct connection to the DCC can be dropped in favour of using the CSMS to relay the arm command to the DCC. Without a measure of this kind, it is difficult to envisage how consumers can control load via the WAN and still comply with the policy findings regarding security and grid stability.

4.6. Local load control supervisor

A logical local load control supervisor would implement the load control arm command coming through from the DCC. This device, a new type of end device within SMETS, would connect to the smart meter Zigbee HAN, implement security measures, receive and translate the arm command before sending it to the EVSE. How the message is formed and interpreted by the EVSE remains to be established. This logical device has some parallels with the SAPC device defined in SMETS and could potentially be the same thing.

For cases when the DSRSP is the originator of the arm command, potentially requiring sub-second response time in order to implement firm frequency response services, the arm command would need to 'pre-authorise' the local load control supervisor to send the arm signal to the EVSE on behalf of the DSRSP. Having been pre-authorised, the local load control supervisor would need to measure the local grid frequency and autonomously send the arm command to the EVSE if the local grid frequency drifted outside defined limits. Although requiring further definition and assessment, this approach could possibly enable the system response time to be achieved while also meeting the policy findings relating to security and grid stability.

Although not directly within scope of this work, it may be worth considering whether metrology should be incorporated into the LLCS for the EVSE specifically for the purpose of settlement of balancing services that may be provided by the DSRSP or virtual lead party within the mechanism of P375. Alternatively this may be achieved directly through an additional SMETS metrology element, either within the boundary meter or through a submetering addition to the SMETS specification.

4.7. DCC and CH / ESAG

The DCC acts as a mechanism for securing load-affecting commands thereby protecting grid stability. It provides all the security features of the smart meter system including anomaly detection, end-to-end security, protocol integrity checking, anti-replay message counters and RBAC to ensure that load-affecting commands reach the intended end point securely. The smart meter communications hub in the premise converts the communications bearer from WAN to Zigbee and allows the local load control supervisor to receive the arm command for implementation on the EVSE. In dwellings where Zigbee communications is challenging, the AltHAN solution can extend the range of Zigbee to practically any required distance. Other WAN and Han solutions, for example broadband / WiFi-based IP communications may also be desirable, although requiring some changes to the existing smart meter architecture. The power saving features of Zigbee would be less relevant to the EV charging scenario as there is no battery-powered gas meter to consider. If the requirements of

PAS1878 were to be implemented in the context of this architecture, then the CH and ESAG may be collocated.

4.8. Central supervisor

The central supervisor fulfils several important security-related functions:

- Central register for all devices, firmware and service providers to be connected to the network
- Associated with a PKI root certificate authority for validation and management of keys and certificates
- Anomaly detection, checking that traffic passing over the network meets security criteria and sending alerts to trigger protective actions (e.g. certificate revovation)
- Secure firmware update service

The central supervisor function has similarities with the DCC and could potentially build on the approach that the DCC has taken for the smart meter system. A degree of re-use of DCC design and even implementation may be possible for selected capabilities, although the specific needs of smart charging, notably the need for innovation, consumer interaction and low latency, must be borne in mind when making such decisions.

5. Conclusion

A variety of options have been proposed to try to explore the benefits and gaps associated with point-to-point and smart meter-based architectures for smart charging. The analysis has shown that uncoordinated point-to-point architectures will struggle to deliver many of the policy findings related to grid stability, cyber security and interoperability. Equally, a pure smart metering approach has limitations in terms of latency, its monopolistic position and perceived ability to deliver innovative, customer-orientated services.

To try to navigate a way through this challenge, a hybrid architecture has been presented which employs the strengths of each to deliver as many of the policy findings as possible. Basing the architecture on point-to-point OCPP communications allows for interoperability of service providers, maintaining competition in the market and avoiding vendor lock-in. Equally, employing the smart meter system for critical load control supervision and provision of smart tariffs seems to play to the DCC's strengths, while avoiding its main weaknesses (whether actual or perceived). Finally, the addition of a new central supervisory function will help to ensure that cyber security and grid stability is maintained.

Clearly, an infinite number of alternative candidate architectures exist and could have been elaborated here and this recommendation may not be the optimum architecture. However, it is hoped that the analysis process has brought some of the key issues to the fore and that subsequent work in this area can improve further on this proposal.

Appendix A. Detailed use case analysis

This Appendix spreadsheet can be accessed via EVEnergyTaskforce.com/reports/phase-two-working-group-3

Or by request **info@evenergytaskforce.com**