Office for Product Safety & Standards

A Study on Developing Options for Assessing Compliance with The Electric Vehicles (Smart Charge Points) Regulations 2021

August 2025

This report was commissioned by the Office for Product Safety and Standards and prepared by TÜV SÜD Ltd.

The views expressed in this report are those of the authors, not necessarily those of the Office for Product Safety and Standards (OPSS) or the Department for Business and Trade (DBT).

Contents

Executive Summary 4

1. Introduction 5

Study objectives and scope 5
Methodology 6

2. Review of best practice and standards 9

Regulations 5 to 11 10
Regulation 12 (Schedule 1) 10
Assessing compliance without standards 11

3. Assessment options 12

Structure 12
Categories 12
Test equipment 14
Smart functionality (Regulation 5) 16
Interoperability (Regulation 6) 16
Loss of communications (Regulation 7) 16
Safety (Regulation 8) 17
Measuring system (Regulation 9) 17
Off-peak charging (Regulation 10) 18
Randomised delay (Regulation 11) 19
Security (Regulation 12) 20
Assurance (Regulation 13) 21

4. Validation of assessment options 22

Procurement of sample 22
Findings 23

5. Challenges with assessing compliance 26

Lack of source code or code execution 26
Limited information in technical file 26
Assessing DSR 27
Implementation of randomised delay 27

6. Conclusion 29

Appendix 1: EVSCP requirements mapped against applicable standards 30

Appendix 2: Stakeholder interview topic guide 46

Appendix 3: Technical file and statement of compliance review checklist 47

Executive Summary

The UK government has introduced legislation requiring Electric Vehicle Smart Charge Points (EVSCP) sold for use in domestic and workplace environments to conform with several functional, security and safety requirements. In 2021, OPSS was delegated as the enforcement authority to ensure compliance with the new regulations.

The primary objective of this project was to provide OPSS with options to assess charge points against The Electric Vehicles (Smart Charge Points) Regulations 2021 when performing market surveillance activity. In doing so, assessment options were developed for each regulation that employed one of five primary assessment strategies, which were then validated and discussed with stakeholders to ensure they were fit for purpose.

Although the Regulations do not mandate compliance with any existing standards, this study identified many standards that could be applied which would result in compliance with specific aspects of the regulations. Where requirements could not be mapped to standards, assessment options were developed based on best practice and industry consultation.

The multiple assessment options available for each requirement should ensure that at least one practical route of assessing compliance can be followed. Alternatively, where the practical assessment can't be performed, or multiple assessments are required, the technical file or other documentation can be used to assess compliance.

During the development of the assessment options, particular consideration was given to the resources and expertise required to implement them. The expense required to purchase the test equipment would be relatively low, with the main costs occurring from power measuring equipment and creating a load for the charge points. The expertise required of the test engineer would be variable, depending on the assessment option and regulatory requirement under test, but it is recommended that they have skills both in cyber security and electrical safety where those requirements are being assessed.

The main foreseeable challenges for the test engineer will come in the form of incomplete documentation or lack of information from the seller regarding Demand Side Response (DSR) emulation and requirements relating to cyber security. Support from the manufacturer for the market surveillance testing would allow for any limitations in documentation to be resolved. The issues surrounding DSR specifically may become less apparent once DSR is commonly implemented across industry, allowing the test engineer to be able to observe DSR communication between the DSR service provider and the charge point. For cyber security, manufacturers could support the test engineer by providing a means of performing code execution for assessing security credentials, access privileges and secure boot mechanisms. Furthermore, if manufacturers are not willing to disclose specific security details in the technical file, they may be willing to provide this information directly to the testing laboratory as part of any market surveillance their charge point may be subject to.

The validation of the assessment options against the two samples was a success, demonstrating that at least one assessment option could be carried out for each requirement. The stakeholders who volunteered through engagement with trade associations, were provided with the opportunity to provide feedback on the assessment options and the overall response was positive, with little feedback on areas for improvement.

1. Introduction

Study objectives and scope

The UK government has introduced legislation requiring relevant Electric Vehicle Smart Charge Points (EVSCP) sold for use in domestic and workplace environments to conform with several functional, security and safety requirements. This legislation came into force on 30th June 2022, with the exception of Schedule 1 which came into force from 30 December 2022, and all applicable electric vehicle charging points sold in the UK from these dates will need to comply with the legislation.

The policy intent of this legislation is to minimise the impact on the existing energy system while charging electric vehicles at home and at the workplace. As the adoption of electric vehicles increases, so does the demand upon the nation's electrical infrastructure. By ensuring that charge points include smart functionality to manage this demand, the cost of upgrading the electricity system will be minimised.

OPSS is the delegated enforcement authority to ensure compliance with the new regulations. The aim of the project was to develop options for assessing compliance of charge points against the regulations.

Objectives

Phase 1 (January 2022 – May 2022)

- To research methods to assess compliance with The Electric Vehicles (Smart Charge Points) Regulations 2021, then report these findings to OPSS and stakeholders of this legislation.
- The TÜV SÜD Ltd team, in collaboration with OPSS and the stakeholders, will develop options for an assessment process that is risk-based, proportionate and consistent. It will be based on best practice principles which include, having a large reach, efficiently and properly evaluated, minimising implementation issues and be effective in meeting the goals of the legislation. The research looks at the requirements from existing best practice, evaluates developing and/or comparable standards applicable to charge points or, where there are gaps based on principles already normalised within design, manufacturing, and testing. This will also be informed by consultations with stakeholders.
- For each requirement, where necessary, describe the appropriate tests, alternative test options and their desired results. In addition, where there are other means to demonstrate conformance (for example, certification against relevant standards), this will be included within the assessment process.

Phase 2 (May 2022 – August 2022)

- To assess and evaluate the various options identified in Phase 1, as well as considering the cost, resources and capabilities to implement them. For example, options could range from a simple visual inspection or documentation, through to light or extensive testing.
- To test and validate the assessment process to identify and address any deficiencies. This will include feedback from the stakeholders.

- To tailor the assessment options towards helping OPSS and charge point stakeholders understand the options for assessing compliance against the regulations.

Scope

- The assessment process relates to the requirements in regulations 5 to 14.
- For regulation 12, the assessment process includes the 11 security requirements detailed in Schedule 1.
- The assessment options include reference to relevant standards where applicable.
- Where it was found that regulations were met as a result of certification to other standards, the assessment process directly refers to this certification as a means of demonstrating compliance.

Methodology

The Electric Vehicles (Smart Charge Points) Regulations 2021 emphasise that the liability is with the seller in ensuring a charge point is compliant at the point of sale:

Sale of charge points

4.—(1) Subject to paragraph (2), a person must not sell, or offer or advertise for sale, a relevant charge point unless—

(a) the relevant charge point complies with the requirements in regulations 5 to 11 of, and paragraphs 1 to 10 of Schedule 1 to, these Regulations; and

(b) the requirements in relation to the sale of a relevant charge point in regulations 13 and 14 of, and paragraph 11 of Schedule 1 to, these Regulations are complied with.

(2) The requirements in Schedule 1 to these Regulations do not need to be complied with in respect of a relevant charge point which is sold before 30th December 2022.

Figure 1 – EVSCP Regulations 2021 – Sale of Charge Points

Assurance

13.—(1) When a relevant charge point is sold, it must be accompanied by a statement of compliance.

(2) A statement of compliance means a document which—

(a) identifies the relevant charge point by reference to its model or type;

(b) contains statements that the relevant charge point complies with these Regulations and that the seller is responsible for ensuring that the relevant charge point complies with these Regulations;

(c) includes the name and address of the seller; and

(d) is signed by or on behalf of the seller and dated.

Figure 2 – EVSCP Regulations 2021 – Assurance

The Automated and Electric Vehicle Act 2018[1] is the primary legislation that grants government the power to regulate charge points 'at the point of sale'. The term 'seller' includes 'letting on hire, lending or giving a charge point', so other scenarios where a charge point is included in the product or service may be in scope of the Regulations.

Although sellers must ensure their goods comply with the regulations, a charge point can only be compliant if the manufacturer designed it with considerations for each requirement. Therefore, for the purpose of this project, the following two stakeholder categories were included as a priority:

Stakeholder Category	Rationale
Manufacturer AND seller of charge points	This stakeholder intends to sell charge points into Great Britain, and therefore is responsible for ensuring the charge points meet the regulations.
Manufacturer only of charge points	This stakeholder does not intend to sell charge points to the end user in Great Britain but is still selling the product to down-stream sellers.

Table 1 – Stakeholders

To ensure a fair representation of the manufacturers included for this project, TÜV SÜD Ltd contacted trade associations and asked them to propose the project to various manufacturers and resellers, asking if they would like to be involved in a one-to-one interview and a stakeholder workshop to discuss the Electric Vehicles (Smart Charge Points) Regulations 2021. As a result, a total of 9 manufacturers and 1 reseller gave their permission to be involved in this project. The primary aim of the interview process was to ascertain stakeholders' interpretation, implementation, and methods of demonstrating compliance against the new regulations. The interviews were held in February and early March 2022. The topic guide used to interview the stakeholders is in Appendix 2.

Throughout the project, research was conducted on applicable standards that can be applied to requirements in the Electric Vehicles (Smart Charge Points) Regulations 2021. Once applicable standards had been identified, these were then mapped against the requirements in the regulations. The results of the mapping process can be found in Appendix 1. Upon completion of the mapping process, various assessment options were developed to assess charge points against the regulations. These assessment options are detailed in section 3. In order to validate the assessment options, test samples were procured from manufacturers for assessment to check the test methods. The results of this validation process can be found in section 4.2.

Stakeholders involved in the one-to-one interview process were invited to take part in a workshop to assess and evaluate the draft assessment options. The workshop was delivered remotely and provided a summary of the project, a breakdown of the assessment options categories, followed by specific details on each assessment option and a deep dive into the practical assessment options. Due to time limitations, the workshop was unable to cover every requirement in The Electric Vehicles (Smart Charge

[1] GOV.UK – The Automated and Electric Vehicle Act 2018

Points) Regulations 2021. The requirements chosen in the workshop were those which required the most analysis and clarification. Throughout the workshop, the stakeholders were asked questions to help prompt feedback on areas of concern around the assessment options.

Input was sought from the following stakeholders as part of this project:

- Trade associations
  - BEAMA: the British Electrotechnical and Allied Manufacturers' Association
  - REA: The Association for Renewable Energy & Clean Technology
  - Energy UK
- Manufacturers who volunteered through the trade associations. It was formally agreed to keep them anonymous due to the nature of the research project and testing involved.

We are grateful to all respondents for their time and insights.

2. Review of best practice and standards

One of the first steps in this project was to map the requirements defined in The Electric Vehicles (Smart Charge Points) Regulations 2021 to those in relevant industry standards and guidelines. During the interview process, stakeholders were also asked which applicable standards they were aware of that could be applied to the regulations. Whilst there is currently no single product-specific standard that comprehensively addresses all the requirements of the regulations, several standards contain elements that align with specific requirements within the regulations. These partial alignments may support compliance with individual regulatory requirements. This feedback, as well as research into the industry and prior knowledge, led to the following standards and guidelines being included in the mapping process:

- PAS 1878:2021 – Energy smart appliances – System functionality and architecture – Specification
- PAS 1879:2021 – Energy smart appliances – Demand side response operation – Code of practice
- ETSI EN 303 645 V2.1.1 – Cyber Security for Consumer Internet of Things: Baseline Requirements
- NISTIR 8259A – IoT Device Cybersecurity Capability Core Baseline
- Code of Practice for Consumer IoT Security
- BS EN 61508-2:2010 – Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
- BS EN IEC 61851-1:2019 – Electric vehicle conductive charging system – Part 1: General requirements
- BS EN IEC 61851-22:2002 – Electric vehicle conductive charging system – Part 22: AC electric vehicle charging station
- BS EN 60529:1992+A2:2013 – Degrees of protection provided by enclosures (IP code)
- EN 62262-2002-07-01 – Corrigendum to EN 50101:1995+A1:1998 – Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code)
- Open Charge Point Protocol (OCPP) v2.0.1 – Parts 0 to 4
- ISO 15118-1:2019 – Road vehicles – Vehicle to grid communication interface – Part 1: General information and use-case definition.
- ISO/IEC 29147-2020 – Information technology – Security techniques – Vulnerability disclosure

The complete results of this mapping process can be found in the appendix.

Regulations 5 to 11

After comparing the requirements in regulations 5 to 11 with existing industry standards and guidelines, it was found that 19 out of 31 requirements could be mapped. The majority of these successfully mapped requirements were found in PAS 1878 and PAS 1879, which is unsurprising given that the regulation was influenced by these two documents.[2] [3]

Outside of the PAS documents, it was found that the Open Charge Point Protocol (OCPP) covered the greatest number of requirements, with 10 requirements being mapped. The following requirements from regulations 5 to 11 could not be mapped to any standard or guideline listed above:

- **Regulation 8** – Safety – 8-2(b)(i), 8-2(b)(ii), 8-2(b)(ii)
  The lack of mapped safety standards or guidelines can be explained by how specific the safety requirements are. Each requirement details the safe override of the default mode of charging, demand side response and random delay, which are all specific features on a charge point.[4]
- **Regulation 9** – Measuring System – 9-2(a), 9-2(b), 9-2(c)
  The measuring system requirements are specific to historic charge data functionality on a charge point.[5]
- **Regulation 10** – Off-peak Charging – All
  All off-peak charging requirements are charge point specific, mostly relating to default charging hours and demand side response agreements.

Regulation 12 (Schedule 1)

After mapping the requirements in regulation 12 (Schedule 1) to the aforementioned standards, it was found that 24 out of 29 requirements in regulation 12 (Schedule 1) could be mapped against a standard or guideline. The Electric Vehicles (Smart Charge Points) Regulations 2021 drew many of the cyber requirements from EN 303 645, and EN 303 645 is based on the Code of Practice for Consumer IoT, which explains the common requirements between the 3 documents. EN 303 645 is also mentioned in PAS 1878, whereby it states “the ESA (Energy Smart Appliance) and CEM (Customer Energy Manager) shall conform to EN 303 645”. Many of the requirements in EN 303 645 which map to the Regulations are ‘recommended’ provisions and are not mandatory for EN 303 645 compliance. Therefore, compliance testing performed to EN 303 645 would not necessarily equate to compliance with all provisions that can be mapped to the charge point regulations.

The following requirements in Regulation 12 could not be mapped to any existing standards or guidelines:

---

[2] It must be noted that the PAS documents are Publicly Available Specifications, these are voluntary as of August 2022 and were mentioned in the government’s summer 2022 consultation, "Delivering a smart and secure electricity system: the interoperability and cyber security of energy smart appliances and remote load control”.

[3] DESNZ & BEIS (2022) Delivering a smart and secure electricity system: the interoperability and cyber security of energy smart appliances and remote load control

[4] Although the list above is extensive, it did not include general electrical or product safety regulations which may be used to demonstrate the safety requirements appropriately.

[5] While not a requirement of the Regulations themselves, compliance with the Measuring Instruments Regulations 2016 (MIR) may be required if the charge point contains a meter that meets the definition of a measuring instrument for the purposes of MIR.

- **Paragraph 12-1** – General Principles – All
  The general principles detailed in requirement 12-1 can be met through compliance to all other requirements in Regulation 12
- **Paragraph 12-8** – Protection against attack – 12-8-3(a), 12-8-3(b)
  These two requirements relate to adequate protection for the charge points user interfaces and attempted use of the charge point other than through the user interfaces
- **Paragraph 12-9** – Protection against attack – 12-9-(a)
  In this requirement, the charge point must notify the owner if there is any attempt to breach the tamper-protection boundary

Assessing compliance without standards

As noted above, certain requirements within The Electric Vehicles (Smart Charge Points) Regulations 20021 could not be mapped to any existing standards. This issue will be addressed by developing assessment options that do not solely rely on the use of standards and are derived from best practice and experience.

3. Assessment options

Structure

The regulations were broken down into 65 unique requirements, and multiple assessment options were written for each requirement.

To streamline the approach and ensure the objectives of the research were being met, the following considerations were given to each assessment option:

- **Equipment required** – Test equipment that could be used to carry out the assessment option.
- **Interaction with seller/manufacturer** – How much interaction OPSS would likely need to have with the manufacturer/seller to carry out the assessment option.
- **Expertise** – The required skillset from the relevant person implementing the assessment option.
- **Time to complete** – An indication of how much time and effort would be required to carry out the assessment option, from 'Very Low' to 'Very High'.
- **Assessment method** – Description on how to perform the assessment option.
- **Pass criteria** – Specific outcomes that must be met.

Categories

Once the structure was in place, multiple assessment options were developed that aligned with the following categories:

- **Technical file review** – In this assessment option, OPSS will be required to request the technical file from the seller/manufacturer if it has not already been supplied with the charge point. In most cases, this assessment option category is expected to take the least amount of expertise and time from the market surveillance team. As part of Regulation 13 (Assurance), the seller/manufacturer is required to create a technical file that includes written descriptions in plain English of the solutions adopted to meet requirements of regulations 5 to 11, and regulation 12 (Schedule 1). Accompanying the technical file shall be written descriptions and explanations in plain English in respect of any diagrams or drawings used in the documentation. Furthermore, the seller is required to include copies of any internal or third-party test reports that are deemed relevant for proving compliance. It must be possible for OPSS to review the technical file and determine whether the charge point complies to each requirement. However, it must be noted that although a technical file template[6] has been provided by OPSS, the sellers/manufacturers are permitted to write the technical file in any format or structure they deem appropriate, as long as it meets the criteria listed in regulation 13.
- **Review of additional documentation or resources –** For this category, where applicable, the test engineer is required to review other documentation outside of the technical file. The test engineer will be instructed to review relevant information within locations such as the user manual, vulnerability disclosure policy, privacy policy or product information on the manufacturer/sellers website. For example, the user manual may contain information about an offline mode, which would indicate

[6] OPSS (2022) EVSCP Regulations 2021 Technical file template

how the charge point is able to charge an electric vehicle even if the communications network is lost (Regulation 7). Additionally, a vulnerability disclosure policy may contain information on how an owner can report security concerns or problems (Regulation 11(2))) or the minimum support period for software updates (Regulation 11(3)).

- **Compliance reports to applicable standards –** In this category, the test engineer can look for specific compliance to applicable standards, such as EN 303 645, NISTIR 8259A or EN 62262. The technical file should indicate which standards have been used to demonstrate compliance, leading the test engineer to request the relevant test report or certificate from the seller/manufacturer. This assessment option specifically allows the test engineer to look for compliance to the provisions which are applicable to the requirement under test. The test engineer is also made aware that an EN 303 645 certificate does not mean that all provisions within EN 303 645 have been met as many of the provisions in this standard are recommended provisions, such as provision 5-12-1 which maps to paragraph 7.1 of the regulations. A test engineer would be required to check for compliance with provision 5-12-1 by reviewing the EN 303 645 test report or the manufacturer's Implementation Conformance Statement (ICS) in combination with a certificate.
- **Assessment performed to an applicable standard –** Where applicable standards exist that align to certain specific requirements of The Electric Vehicles (Smart Charge Points) Regulations 2021, it is possible that some manufacturer/sellers will not have used them to achieve compliance. In this instance, as part of any market surveillance, OPSS can use these applicable standards as a method of carrying out testing on a test sample. For example, where a provision in EN 303 645 is applicable to the relevant requirement, the test engineer can use TS 103 701 as a test method. TS 103 701 is a technical specification that details how to carry out testing to EN 303 645. If using TS 103 701, the test engineer will be required to ask the manufacturer/seller to complete the Implementation eXtra Information for Testing (IXIT), which is a self-declaration form defined in the technical specification. The assessment option will specifically state which entries within the IXIT are required to be filled for each requirement in The Electric Vehicles (Smart Charge Points) Regulations 2021. This will save the manufacturer/seller from filling in the entire IXIT. Once the test engineer has received the completed IXIT, the testing process outlined in TS 103 701 can be followed.
- **Practical assessments –** This category involves the practical assessment of a test sample using a method that is not based on any test standard. Instead, the assessment is derived from best practice and experience to assess compliance to the requirement. Most of the assessment options in this category are conducted independently of the manufacturer/seller and are performed from a 'black box'[7] pproach. However, for some requirements in Regulation 12 (Schedule 1), the assessment options ask for code execution to be provided on the device under test, or for a firmware sample to be provided for the test engineer to unpack and analyse. Without this, it can be difficult to practically assess requirements such as security credentials stored on the device (Regulation 12 – Schedule 1 paragraph 4(1)) or

[7] Black-box testing is a type of software testing in which the tester is not concerned with the software's internal knowledge or implementation details but rather focuses on validating the functionality based on the provided specifications or requirements. www.geeksforgeeks.org/software-testing/software-engineering-black-box-testing/

checking for any unnecessary software services running (Regulation 12 – Schedule 1 paragraph 9(d)). Most of these assessments are rated as 'High' or 'Very High' in terms of the time to execute the method, and the amount of expertise required can be quite demanding, varying from electrical safety knowledge, to experience in cyber security testing. By contrast, assessments involving the verification of test sample functionality are elementary and less demanding on test engineer expertise, such as pre-set default hours (Regulation 10(1)) or information provided to the owner relating to historic charge data (Regulation 9(2)).

Test equipment

For the practical assessment options, there are instances where test equipment is required to carry out the test method. All measuring equipment shall be calibrated according to ISO 17025 to ensure the results are accurate and repeatable. The identified test equipment includes the following:

Measuring power

Option 1 –

- **Power analyser** – This is used to perform current, voltage and power measurements. It is useful for any of the requirements in the regulations relating to power measurement (e.g. Regulation 9(4)(a)) whereby the power measured by the power analyser can be compared to the power measured by the meter on the charge point. A breakout box will need to be installed to gain access to the live wires going into the charge point. This solution will record both the power delivered by the charge point, and also the power used by the charge point for its operation. Therefore, the power will need to be measured while the charge point is idle and then this value is to be subtracted from the final power measurement. As charge points found in domestic and workplace environments can use three phase power, a power analyser that supports three phase power measurements would be required to test such devices. 3-phase power analysers typically vary from £1,000 to £6,000.

Option 2 –

- **Current clamps –** As an alternative to a power analyser, current clamps can be used to measure the current of output of the charge point. Current clamps must be placed around the outside of the live wires coming out of the charge point, which may require the charge point casing to be opened to gain access. Solutions chosen by manufacturers to meet the tamper protection boundary requirement, may mean the charge point does not function when the casing is opened. In this case, the live wires going into the charge will need to be accessed. Current clamps typically cost between £50 and £200.
- **Voltage probes –** In order to calculate power using the current clamps above, voltage probes will also be required, as power is a measurement of current and voltage. Voltage probes typically cost £20 to £100.
- **Data logger –** The current clamps and voltage probes will be continuously measuring current and voltage. To support 3-phase power calculations, each phase will need to be measured, requiring 3 voltage probes and 3 current clamps. All 6 measurements can then be logged using a suitable data logger to calculate the final power consumption. This power measurement can then be compared with the power measured by the meter in the charge point. A suitable data logger with the required number of channels is approximately £1,500.

Connecting a load

Option 1 –

- **Electric vehicle –** In order to measure the power output of a charge point, a load is required to draw the power from the charge point. One option is to use an electric vehicle to create this load. This can be a cost-effective option if there is already an electric vehicle ready to use at the testing facility. However, if using an electric vehicle, the charge would need to be discharged before it could be used to draw power from the charge point again. The location of the vehicle in relation to the testing laboratory will also need to be considered.

Option 2 –

- **Electric vehicle supply equipment (EVSE) tester –** Some EVSE testers include a socket for the connection of an external load to test the performance of the power meter and can also simulate different current capabilities and charging rates. They typically cost between £400 and £700, and require the use of a multifunction tester to connect to the terminals on the EVSE tester.
- **Variable 3-Phase load –** As mentioned above, an external load can be connected to a compatible EVSE tester to draw power from the charge point. The load will need to simulate different charge rates that an electric vehicle could request from the charge point and must be able to support 3-phase and a minimum of 22kw. They typically cost between £4,000 and £10,000, although some sellers provide an option to loan. Such loads can generate vast amounts of heat and noise, which can impact working conditions in a small testing laboratory with this solution, there is no need to discharge a battery.

As well as measuring equipment, the test engineer will also require mechanical impact test apparatus if they are verifying or assessing the IK code rating according to EN 62262. This will consist of either a pendulum hammer, free faller hammer or steel weights, all of which should be calibrated to ensure 5 joules of energy is applied when striking the charge point.

The practical assessment options also require the use of software to test the Regulation 12 (Schedule 1) requirements. A typical setup would include a test computer connected to the same wireless access point as the charge point. This computer can then be used to run various programs such as a network protocol analyser (e.g. Wireshark) for monitoring the network traffic to and from the charge point; a network scanner (e.g. Nmap) to identify any open network ports on the charge point; a firmware analysis tool (e.g. Binwalk) to unpack and inspect firmware samples; and brute forcing[8] software to attempt to identify any weak authentication passwords on the charge point. Should the charge point not communicate over Wi-Fi, specific equipment would be required to sniff (analyse) the data coming to and from the charge point. For example, if the charge point supported Zigbee, a Zigbee sniffer would be required.

The next section of the project was for TÜV SÜD Ltd to devise various assessment options for how a charge point could be assessed against each of the regulations. This covered Regulations 5 to 11, Regulation 12 (Schedule 1) and Regulations 13 and 14.

[8] A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. What is a Brute Force Attack? Definition, Types & How It Works | Fortinet

Smart functionality (Regulation 5)

The requirements in Regulation 5 address “Smart functionality” of charge point devices, with the functionality enabled by network or internet connectivity. A significant aspect of Regulation 5 is DSR (Demand Side Response) and response DSR services. DSR is routine DSR implemented through supplier set electricity tariffs or other electricity related incentives. Response DSR is initiated at the request of regulated electricity participants, often in near real time, to help balance demand. Ensuring that all charge points support DSR and response DSR is intended to help protect the demand on the grid, which is especially important as the usage of electric vehicles increases.

Many of the requirements in Regulation 5 are easy to assess and limited input from the manufacturer/seller may be required. The smart functionality supported by the device can be ascertained from reviewing the user manual or observing the features available within the user interface, such as a mobile application or companion device. From a practical perspective, when installing the charge point, the test engineer can check there is a step to connect to a communications network, whether that be a WiFi network, 4G network or so on. Once installed, the test engineer can attempt to remotely control the charge point to initiate a charge or change the rate of charge.

When assessing compliance with Regulation 5, validating the presence and functionality of the response DSR will pose the greatest challenge. The test engineer can review the technical file, which must describe the solution adopted to meet Regulation 5 but it will be a challenge to practically observe response DSR in a test lab environment. To observe response DSR behaviour, a DSR service provider will need to communicate directly with the test sample, or a manufacturer will need to provide a means of emulating response DSR messages for the test engineer to check that the charge point is responding correctly. Some of the challenges and potential upcoming solutions for assessing DSR can be found in section 5.3.

Interoperability (Regulation 6)

Regulation 6 ensures that an owner can change electricity supplier without losing the smart functionalities described in Regulation 5. If owners have charge points which no longer support smart functionality due to an energy supplier change, it would impact the overall intent of the Electric Vehicles (Smart Charge Points) Regulations 2021, which is to protect the electricity grid from an excessive increase or decrease in demand. From an assessment perspective, the support for this regulation can be judged by checking there is no dependency on an electricity supplier when purchasing and installing a charge point. Therefore, the practical assessment here would be to go through the steps involved in the purchase, registration, and installation to check at no stage the owner is required to disclose their electricity supplier. If they do have to disclose it, the manufacturer will need to be contacted to find out what impact that disclosure would have on interoperability. In a testing environment, it is not practical to change electricity supplier to prove smart functionality still exists. There is no specific expertise or test equipment required for this assessment.

Loss of communications network access (Regulation 7)

As described in Regulation 5, all charge points must be able to connect to a communication network. However, there will be times when a communication network is not available, such as when charge points are installed in areas where there is no network

connection available, or when there are technical issues with the owner's internet service provider that temporarily prevents access to the internet. In the event that a communication network is not available, it is important that the primary functionality of the charge point still exists, which is to charge an electric vehicle.

Assessment of a charge point's ability to charge without a network connection will be simple. There may be reference to an offline mode in the technical documentation which states the charge point can charge an electric vehicle while not connected to a network.

To practically assess this requirement, the test engineer will be required to disable or disconnect from the communications network and check that the charge point can still charge an electric vehicle. A means of connecting a load to the charge point will be required for this assessment, whether that be an electric vehicle or a load that is connected via an electric vehicle supply equipment (EVSE) tester.

Regulation 7 can be mapped to recommended provision 5.9-2 in EN 303 645, which states "Consumer IoT devices should remain operating and locally functional in the case of a loss of network access…" If a charge point is compliant to provision 5.9-2, then the charge point is also compliant to Regulation 7. If compliance to 5.9-2 has not been provided, the test engineer could use the test steps outlined in TS 103 701 that relate to a loss of network as a way of assessing compliance to Regulation 7.

Safety (Regulation 8)

Regulation 8 relates to how a charge point is configured to prevent there being a risk to the health or safety of persons while overriding the default mode of charging, provision of DSR services, and random delay. The intent of this is to ensure that manufacturers have considered safety when modifying or upgrading their charge points to meet these regulations, and that existing baseline device safety requirements have not been compromised.

Although the overriding of these specific functions on the charge point cannot be mapped to any relevant safety standards, there are safety standards such as BS EN 61508-2 and BS EN IEC 61851 that consider the safe operation of the device in all functional states. Therefore, evidence of compliance to a safety standard could be a way of demonstrating compliance with this requirement. In this scenario, the test engineer is to review the relevant safety test reports to check the charge point conforms to Regulation 8.

The technical file may reference a failsafe mode (Mode 4), as described in section 5.3.5.2.5 of PAS 1878. If implemented correctly, it should not be possible for the owner to perform any consumer override functions when the device is in failsafe mode, as illustrated in 'Table 1 - Operating modes' of PAS 1878. The test engineer should have a good understanding of electrical safety and relevant standards to help understand whether the information in the test reports or technical file demonstrate the charge point meets the three safety requirements in the regulations.

Measuring system (Regulation 9)

Accurate reporting of how much electricity is being used by charge points is vital for an efficient use of response DSR (Demand Side Response) services, allowing DSR service providers to react quickly to protect the grid where necessary, as well as to enable visibility to the consumer of the electricity used to charge their vehicle.

As most of the requirements within Regulation 9 are related to the functionality, including how the historic charge data can be provided to the owner, the compliance of the charge point can be verified by checking the technical file. If not using documentation, a review of the charge points functionality via its interfaces will quickly inform the test engineer how historic charge data is displayed to the owner.

While not a requirement of the Regulations themselves, compliance with the **Measuring Instruments Regulations 2016 (MIR)** may be required if the charge point contains a meter that meets the definition of a measuring instrument for the purposes of MIR. If MIR compliance is being used as a means of meeting the measuring system requirements, then the MIR test report would be available as part of the technical file.

The measurement accuracy of the charge point can be practically assessed through the use of specific measuring equipment, all of which should be calibrated according to ISO 17025. Through use of current clamps, voltage probes and a logger, the power output from the charge point can be determined. Alternatively, a power analyser can be used to calculate the power. Once the power has been measured over the duration of 1 hour, this value is then compared against the reported power measurement on the charge point to calculate its accuracy. Identifying whether the inaccuracies are systematic can be practically assessed by measuring the accuracy of additional samples to check that they do not have the same inaccuracy. If for example sample 1 had a measurement inaccuracy of +9%, sample 2 had +8.7% and sample 3 had +9.1%, a consensus could be drawn that the inaccuracies are systematic, and therefore fails the requirement. Ideally, all samples should have accuracy measurements that are significantly different, unless all measurements are close to 0%, such as ± 1%. Alternatively, the test engineer can look at the systematic inaccuracy of various power measurements on one sample. In this scenario, the power would be measured at various load points, including 25%, 50%, 75% and 100% load. A weighted mean error (WME) calculation is then performed to check it is within the appropriate tolerance levels.

Practically assessing that the charge point has a sampling rate of at least 1 second could be challenging. One option is to review the circuit diagram or technical drawings (and written descriptions if referring to the technical file) to identify how the charge point measures the power output. Once the measuring component has been identified, the signals from the component to the CPU (Central Processing Unit) can be monitored using an oscilloscope to ascertain those measurements are being made at least once per second. However, although the CPU may be receiving signals at a frequent enough rate, it does not necessarily mean the software processes this information once every second. Alternatively, the test engineer can research the sampling rate of the specific measuring component used within the charge point, or review the historic charge data to check it can be displayed in 1 second data points.

Off-peak charging (Regulation 10)

By default, the charge point shall be configured to have pre-set default charging hours which are outside of peak hours. The owner must be given the opportunity to accept the pre-set default charging hours; to remove the pre-set default charging house or to change these default charging hours upon first use and any time after it is first used. The owner must also be able to override default charging modes and DSR services. The intent of these requirements is to give the owner full control over when a charge point charges an electric vehicle, while also limiting the burden upon the electrical grid at peak times.

The assessment of these requirements can be done by checking the functionality supported by the charge point in either the technical file or other available documentation. A practical assessment can be performed by reviewing the required functionality upon first use and after first use. No specific test equipment is required for assessing the requirements in Regulation 10, other than a means of connecting a load to the charge point to be able to check that the test engineer can override the provision of DSR or the default mode of charging. It may prove to be difficult to demonstrate that DSR services can be overridden without signing up to a DSR agreement that has time of use tariffs that will ensure DSR services are activated at specific times. If the test engineer wishes to test whether response DSR services can be overridden, they would need a means of initiating response DSR services, which may require the assistance of the manufacturer or DSR service provider.

Randomised delay (Regulation 11)

To help maintain grid stability, the Electric Vehicles (Smart Charge Points) Regulations 2021 include randomised delay requirements to help reduce the amount of charge points starting a charge or changing their rate of charge simultaneously. The randomised delay is to occur any time electricity starts flowing through the charge point for the purpose of charging a vehicle, or increases or decreases. The randomised delay should not occur when the charge point is in DSR response mode to allow for the DSR service provider to have control over exactly when charge points are turned on, up or down. This delay is applied to the time when the charge begins and should not affect the duration of a charge. By offsetting the start of each charge randomly, a disruptive scenario where all charge points begin charging at the same time can be prevented. During the stakeholder workshop, some stakeholders said that they intended to implement the randomised delay functionality at the end of a charge, to prevent a sudden drop in demand, which could be as damaging to the grid as a spike in demand.

The majority of the randomised delay requirements can be assessed by reviewing the functionality supported by the charge point, such as observing the randomised delay before the charge point starts charging, or the option to cancel a randomised delay.

There is one requirement that states the maximum duration of the delay must be able to be increased or decreased remotely via a communications network. However, it should not be possible to change the maximum randomised delay to be below 600 seconds. The test engineer will need to contact the manufacturer or charge point operator to ask them to change the maximum randomised delay. Unfortunately, it may not be possible for the manufacturer to update the maximum randomised delay on the one specific charge point being tested, and therefore may not be willing to change the randomised delay because it may impact all charge points connected to their server. In this scenario, a review of the technical file can be used as a basis of checking the charge point supports the ability to remotely change the maximum delay.

Assessing the randomness of the delay values can be achieved by performing a runs test on a large sample size of randomised delay measurements. A runs test is a statistical test used to determine whether the data obtained from a sample is random.

Security (Regulation 12)

Regulation 12 is defined in Schedule 1, and all requirements in Schedule 1 are related to the security of the product. As all charge points sold after the regulations come into force should be internet connected, it is important that the charge points have a good level of cyber security to prevent and mitigate risks of unauthorised access causing harm to either the owner, charge point, cloud servers or the electrical grid.

The security requirements are split into the following sections in Schedule 1:

- **General principles**
- **Passwords**
- **Software**
- **Sensitive security parameters**
- **Secure communication**
- **Data inputs**
- **Ease of use**
- **Protection against attack**
- **Security log**
- **Provision of information**

As mentioned previously in this report, many of the requirements found in Schedule 1 can be mapped to EN 303 645. Therefore, a simple approach to checking compliance for the mapped requirements is to review EN 303 645 test reports and assess which provisions are compliant. Where there is no evidence of compliance to EN 303 645, the test engineer can carry out TS 103 701 as a means of testing the provisions in EN 303 645 that map to the requirements in Schedule 1. The TS 103 701 test process requires the manufacturer to complete an Implementation Conformance Statement (ICS) and an Implementation eXtra Information for Testing (IXIT). There are currently no templates provided by ETSI for either of these documents. The templates will have to be created by either the testing laboratory or manufacturer. Considering the substantial technical expertise and effort required to complete an ICS and IXIT, the test engineer may not receive a complete ICS and IXIT and therefore be unable to apply tests based upon review of these documents.

Another similar approach to assessing the security requirements is to review the information found in the technical file. The technical file must describe how each requirement is met, such that the enforcement agency, OPSS, must be able to ascertain if a charge point is compliant by reviewing the technical file alone. A non-exhaustive list of examples of how technical requirements have been met are: the implementation of software update mechanisms, methods of encryption used to communicate with the cloud server and how passwords are generated to ensure they are unique per device.

From a practical assessment perspective, the assessment options are derived from conventional methods used in penetration testing and security assessments of IoT products. The test equipment required to conduct the assessment options include, but are not limited to, brute forcing[8] software to identify any weak default passwords, a network protocol analyser for observing network traffic to and from the charge point, a network port scanner to identify any open UDP (User Datagram Protocol) or TCP (Transmission Control Protocol) network ports and fuzzing software to investigate the charge points input validation methods. For some practical assessment options, the manufacturer must provide a firmware sample or guidance describing how to obtain the firmware from the test

sample. By doing so, the test engineer can unpack the firmware and uncover security-relevant artifacts such as password hashes, security parameters, software versions and device configuration files, which could then be used to indicate compliance with these regulations.

The test engineer can also perform a hardware assessment on the charge point. This will involve removing the outer casing of the charge point to look for any signs of tamper protection mechanisms or exposed debug interfaces. If an exposed debug interface is found, such as a UART, JTAG or USB port, the test engineer can attempt to connect to them to verify whether they have been disabled. For the most in-depth practical assessments, the test engineer can ask the manufacturer for the source code and perform a source code analysis to check for any hard-coded security credentials.

For the requirement related to protection against physical attack, the test engineer could perform impact protection testing in accordance with EN 62262 against each external face of the charge point to verify it has an IK rating of at least IK08. Test equipment such as a pendulum hammer or a free fall hammer are required to perform such impact tests.

An extensive review of the manufacturers vulnerability disclosure policy, privacy policy and user manual are included in the assessment options. This is primarily to assess the requirements related to how an owner can delete personal data, how vulnerabilities can be reported, the support period of the product and how to setup the product securely.

Assurance (Regulation 13)

Regulation 13 (Assurance) describes the required contents of a Statement of Compliance (SoC) and Technical File. As mentioned previously in this report, there is no strict format on how a manufacturer/seller is to complete these documents. Prior to performing any of the assessment options, it is important to check that all documentation is available and contains the correct information to be compliant to Regulation 13, as incomplete assurance documentation could mean the sale of a charge point is also a breach of Regulation 4 which prohibits the sale of non-compliant charge points. As a method of checking the Statement of Compliance and Technical File, a checklist has been created that allows a test engineer to ensure that all the relevant information is present while performing a review of the documentation. This checklist can be found in the Appendix 3.

4. Validation of assessment options

This section contains information on how the assessment options were validated, including how the samples were procured, and what were the findings when applying the assessment options against the test samples.

Procurement of sample

During Phase 1 of the project, suitable charge points were investigated that could be used for validating the assessment options against a test sample. A suitable charge point would ideally contain all functionality required for the complete assessment of the EVSCP Regulations, such as a DSR or randomised charging delay. As no charge points were found with all of the functionality required due to the time of this research being prior to regulations coming into force, the next step was to identify if the charge points met the following criteria:

- **3-phase power support –** Although uncommon, some domestic and workplace chargers can support up to 3-phase 22kw power output. Therefore, it would be optimal to validate the assessment options against a charge point with the highest possible power output.
- **Smart connectivity –** Without Smart connectivity, most of the functionality covered by the regulations will not be met, and therefore, many of the assessment options can't be performed.
- **Type 2 connector and mode 3 charging support** – Type 2 connectors and Mode 3 charging are the most common for domestic and workplace chargers that are applicable under these regulations.
- **Over the air update support –** Support for software updates will allow the update mechanism to be assessed in accordance with the regulations.
- **Charge schedule –** If the charge point supports features relating to the setting of charging schedules, it will allow the test engineer to investigate the functionality surrounding pre-set charging routines.

The initial intention was to purchase a sample from a manufacturer or retailer from the route of a consumer, but it became apparent this was not the most beneficial approach. As many of the assessment options require collaboration with the manufacturer, which would be necessary for obtaining the technical file, additional documentation, firmware samples or for providing guidance to simulate functionality such as the response DSR service. For this reason and given that manufacturers were already aware of this project during the interview process, some manufacturers were contacted to ask if they would like to provide a test sample to be validated against the assessment options. The manufacturers were advised of the intentions of the project, and it was made clear that the charge points would remain anonymous.

Two manufacturers volunteered and provided test samples to be tested using the assessment options. Both manufacturers mentioned that their samples did not yet meet the new regulations and were still developing updates to address non-compliant aspects of their products as this was prior to the regulations coming into force.

Fortunately, the provided test samples represented a diverse range of charge point use-cases and implementations. Sample 1 was a single-phase charger designed for both home and workplace environments, whereas Sample 2 was designed primarily for home use but supported three-phase as well as single-phase power. Furthermore, Sample 1 supported ethernet connection, whereas Sample 2 used Wi-Fi, allowing the evaluation of the developed assessment options with several methods of network communication.

Findings

The next step in the project was to validate the assessment options against the samples provided by the manufacturers. Installation of the test samples was performed by TÜV SÜD Ltd using the installation guides provided with the charge points.

Sample 1 was provided with a technical file. This technical file was based upon the template publicly available from OPSS[9] and was a draft document. Sample 2 did not have a technical file available.

Each assessment option was validated by applying the associated methodology to both test samples, where any limitations in the assessment option or unforeseen edge-cases in the test sample implementation would become apparent. The general outcome of this validation process is broken down as follows:

Assessment Option 1 – Technical file review

Using the draft technical file provided with sample 1, the document was reviewed in its entirety to assess whether the charge point complied to each requirement. Due to the brief answers provided throughout the technical file, it proved difficult to make any determination of whether the stated technical solutions were compliant with their relevant requirements.

The technical file frequently referenced the Open Charge Point Protocol (OCPP) as a means of compliance but did not specify the OCPP requirement or feature that would map with the relevant EVSCP requirement. Although 10 EVSCP requirements were identified in this report that could be mapped with OCPP, a test engineer would need a test report or similar proof of OCPP compliance to make a determination of compliance with the EVSCP requirements. However, although this charge point supports OCPP, it could not be found on the list of approved devices on the OCPP's list of certified products. Given that there is a range of OCPP compliance levels (Full, Security and Subset), a charge point may implement OCPP and lack all the features and requirements detailed in the OCPP, including those mapped with EVSCP requirements. For this reason, stating compliance via OCPP in the technical file is not sufficient and further information would be required to confirm which parts of the OCPP the charge point is compliant to. In such cases, the test engineer would need to review an OCPP test report to inspect which elements of the OCPP are supported by the charge point.

A review of the technical file also found answers which solely claimed compliance, as opposed to describing the technical solution adopted to meet the relevant EVSCP requirement. Furthermore, where a requirement contained multiple sub-requirements, it was found that many of the stated technical solutions and answers only addressed the first element of the legislation text. It must be noted that the technical file was still in draft form, but this validation process has further raised concerns that technical files may often lack

[9] DESNZ, OZEV & OPSS (2022) Guidance - Regulations: electric vehicle smart charge points

the required details to determine whether the technical solutions adopted to meet the requirements are appropriate.

Assessment Option 2 – Review of additional documentation or resources

This assessment option presented opportunities to obtain information without the need for installation or operation of a charge point. Both test samples were provided with user manuals and installation guides, allowing the test engineer to assess the various functionality supported by the device.

Upon review of the manufacturer's websites for data privacy and technical specifications, test engineers were only able to find a Vulnerability Disclosure Policy (VDP) for Sample 1. Assuming the manufacturer for Sample 2 does not have a VDP, it is expected that one will be created before the schedule 1 requirement mandate.

Other than the VDP, the most noteworthy absence from the documentation was information regarding the DSR and randomised delay, meaning that test engineers were unable to determine a verdict for these requirements for this assessment option.

Assessment Option 3 – Compliance reports to applicable standards

Standards such as BS EN 61851-1 were referenced in the documents supplied with both test samples, however, there were no compliance test reports provided with either sample. Without test reports, it would not be possible to make any determination of compliance with EVSCP requirements and so it was not possible to validate these assessment options.

Assessment Option 4 – Assessment performed to an applicable standard

This assessment option involves the application of test methodologies defined for standards which were mapped with EVSCP requirements. As the standards chosen for mapping are already considered valid and effective, any validation of the test methodology itself would yield no value and be duplicative. Furthermore, test specifications such as TS 103 701 require the manufacturer to complete extensive self-declaration documents, which is a significant undertaking for the mere purpose of validating already proven standards. As a result, assessment option 4 was excluded from this validation.

Assessment Option 5 – Practical assessments

Validation of assessment option 5 was the most crucial as it involved practical assessment and would prove to be the most strenuous. Both test samples were still in development, meaning that some functionality had not yet been implemented, including features relating to Schedule 1. As a result, there were several areas where the charge points did not comply to the regulations, such as the operation of randomised delay, tamper protection and DSR.

One area where this validation process identified issues in the testing methodology was the assessment of randomised charging delays. Sample 1 did not yet support randomised delay, but Sample 2 had implemented it. Before the samples were provided, it was anticipated that the charge point would display the randomised delay in a manner that test engineers could accurately record, such as a countdown on the user interface or a status indicator. However, Sample 2's implementation of a randomised delay meant there was no indication to the test engineer when the randomised delay was occurring. The randomised delay occurred at the beginning of a scheduled charge, but the clock time set on the charge point was not visible, preventing the test engineer from observing the moment

when the delay had started. Furthermore, there was no visual indication of any form to illustrate that the randomised delay was taking place. Also, the charge point did not support a randomised delay at the beginning of manual charging cycles, which is non-compliant with requirement 11-2(a), which specifies that the randomised delay is to occur each time electricity starts flowing through the charge point. If the charge point had supported a randomised delay on manual charge cycles, the test engineer could have measured the time between initiating the manual charge and the start of charging, to record the randomised delay. Sample 2 also presented additional challenges in verifying the maximum randomised delay value, and whether that could be increased or decreased. There was no mention of the randomised delay in the user manual or the settings within the user interface, and so no option to view or change the maximum randomised delay period was available to the test engineer. In this scenario, the test engineer would be reliant on either self-declaration from the manufacturer, or information in the technical file to confirm the capabilities surrounding the maximum randomised delay value. The method of measuring the randomised delay or assessing the maximum delay value will vary depending on the charge point's implementation.

During the stakeholder workshop, there was no feedback regarding the use of the Runs Test as a method of determining whether the randomised delay values were random, but there was consensus that there was no entropy or randomness requirement and only that charging delays are not predetermined. Therefore, a Runs Test can be considered as a suitable method of assessing that the randomised delays are not predetermined, but due to the issues of measuring the randomised delay values during this validation process, the runs test could not be used.

Neither sample had any active support for DSR or DSR agreements. The DSR testing was expected to be a challenge when drafting the assessment options, and this validation exercise has further reiterated the issue. Sample 1 was stated to be compliant to DSR due to its support for OCPP, but there was no evidence to suggest that DSR messages were being communicated with the charge point during testing. Therefore, until DSR becomes an active feature on the charge points, the test engineer will have to rely on the technical file for confirmation that the charge point is capable of supporting both DSR and response DSR.

Validation of the tamper protection boundary assessment options also yielded unexpected results. The technical file for Sample 1 mentioned that tilt sensors were in place, but during a hardware assessment there was no evidence of any tilt sensors when inspecting the internals of the charge point. When designing a charge point, it is logical for the manufacturer to disguise or hide the tamper protection sensors to make it more difficult for an attacker to bypass; however, while the charge point was in operation, the test engineer was unable to activate the tilt sensors by moving the charge point through different angles. As the test sample was pre-production, it is likely that the tamper protection mechanisms may not be implemented or fully functional yet, and not a concern with the assessment method itself.

With exception of assessment methods that required source code or code execution on the device, all remaining practical assessments were conducted as expected and without issue. For further details on source code or code execution, see section 5.1. The test equipment used to measure the power accuracy and simulate the load worked as intended. Where necessary, minor modifications were made to the assessment methodology to help streamline the testing during any market surveillance performed by OPSS.

5. Challenges with assessing compliance

In all, the validation of the proposed assessment options proved successful. Despite limited support and available documentation, it was always possible to perform at least one assessment option for each requirement on both samples. When stakeholders were provided with the opportunity to provide feedback on the assessment options, the overall response was positive, with little feedback on areas for improvement.

However, despite the positive outcome of the validation process and stakeholder workshop, some challenges still occurred with assessing compliance to the regulations. A summary of these challenges can be seen below:

Lack of source code or code execution

For the two procured samples, neither manufacturer provided source code or any means of performing code execution. This meant that the some of the cyber security requirements in Schedule 1 were difficult to practically assess, such as evaluating security credentials or secure boot mechanisms.

Limited information in technical file

The technical file that was provided with sample 1 contained very brief answers that made it difficult for the test engineer to evaluate whether the charge point was compliant to the regulations. During the stakeholder workshop, manufacturers raised concerns over the amount of information provided in the technical file, especially relating to the cyber security requirements[10]. The manufacturers were encouraged to try and provide as much detail as possible, thus enabling a test engineer to review the technical file and assess whether the charge point meets the requirements, and to ensure they did not inadvertently breach regulation 4. The following example was provided to help explain this point:

Requirement: A relevant charge point must be configured so that communications sent from it are encrypted.

- Technical file example 1: *"All communications sent from the Charge Point to its associated cloud services are encrypted"*

While this answer claims compliance with the relevant requirement, it lacks implementation details that would allow a test engineer to infer if compliance had been met

- Technical file example 2: *"All API communication from the Charge Point to its associated cloud services is sent using TLS 1.2. The Charge Point also uses a proprietary protocol to communicate with a LAN charge controller, which is encrypted using AES-256 CBC."*

This second answer would be suitable as it describes the encryption methods being used and the remote services being communicated with. However, as pointed out by the manufacturers, providing too much information in the technical file can potentially help an attacker expose vulnerabilities on the charge point as this information would be available to the purchaser on request. For example, if a manufacturer described details of the tamper protection mechanisms being used and where the tamper protection boundary is

[10] Regulation 13 of The Electric Vehicles (Smart Charge Points) Regulations 2021 requires the technical file to be available to the buyer upon request.

located, this would help an attacker bypass the tamper protection mechanisms. As a result, the manufacturers will need to carefully balance the need to provide enough information to satisfy requirement 13 whilst protecting intellectual property and any information that could be useful to a hacker to bypass security mechanisms.

Assessing DSR

The implementation of DSR is currently non-standardised, with manufacturers opting for many different routes of implementing DSR and response DSR. This lack of standardisation proves to be a great challenge when assessing compliance. The assessment method relating to DSR, specifically emulating response DSR, was presented for stakeholders to discuss how they internally test their devices to ensure compliance with this requirement. Generally, manufacturers claimed limited capability to emulate response DSR signals to the charge point, despite the growing prevalence in electric vehicle supply equipment (EVSE) industry.

Although the charge points themselves can be capable of response DSR through implementation of the Open Charge Point Protocol (OCPP), without being able to emulate response DSR messages, it will be a significant challenge for test engineers to practically validate compliance for response DSR. There are currently trials taking place for DSR services, so assuming they become pervasive across the entire EVSE industry, it may then be achievable to observe response DSR in real time while assessing a charge point. Furthermore, there is currently a flexibility innovation programme, which involves laboratory testing and demonstration of interoperable DSR applications in settings indicative of the real world.

Although the protocol used for DSR is not yet regulated, PAS 1878 outlines the OpenADR (Open Automated Demand Response) protocol as a candidate for a standardised approach for interoperable communication between the DSR service provider and the customer energy manager (Interface A). This interface is vital for receiving reliable information from potentially millions of devices to help understand the electrical demand on the grid at any moment in time. Should this interface be compromised, an attacker could initiate a spike or drop in demand by controlling how and when the charge points are charging an electric vehicle, which may cause significant implications on the national grid. Therefore, the importance of being able to assess the accuracy and stability of the communication between the charge points and the DSR service provider cannot be underestimated. The outcome of this project may yield a standardised approach on how interoperable response DSR can be assessed against PAS 1878 (Stream 1). Also noting that through the IDSR innovation programme (part of the flexibility innovation programme) this will look to also create a test specification for PAS1878.[11]

Implementation of randomised delay

As identified during the validation of the assessment options, the lack of visual or audible indications of the randomised delay meant it was not possible to accurately measure the randomised delay to the nearest second for scheduled charges. If other manufacturers also adopt this same implementation, OPSS may have difficulties confirming a charge point is compliant with the randomised delay requirements.

[11] DESNZ & BEIS (2022) Flexibility Innovation Programme: Laboratory testing and demonstration of interoperable DSR applications

The subject of randomised delays was discussed during the workshop, most notably the interpretation of the requirement rather than the test methodology. Stakeholders were mostly concerned with the poor customer experience that a randomised delay will introduce, as well as clarity on when randomised delays should occur, such as at the end of the charge cycle or when the charge cycle has been initiated manually. The assessment methodology mentions that the user should not be able to change the maximum randomised delay value as this could lead to owners trying to set the randomised delay value to a minimum.

Some manufacturers mentioned in the workshop that their charge points supported either a global override that allowed the randomised delay to be disabled by a third-party, or a feature that allowed the user to disable the randomised delay. Such implementations of the randomised delay would not have the positive impact on the grid intended by the functionality, and would fail to meet the policy intent of the regulations. Further, if the owner of the charge point is not able to cancel the randomised delay at each charging instance, it would fail to meet the criteria set out in the assessment options.

6. Conclusion

The creation of the assessment options has helped OPSS develop their path to assessing compliance against The Electric Vehicles (Smart Charge Points) Regulations 2021 as part of the market surveillance strategy.

The five assessment option categories consist of:

1. a technical file review;
2. review of additional documentation or resources;
3. compliance reports to applicable standards;
4. assessment performed to an applicable standard; and
5. practical assessments.

For the practical assessment options, there are instances where test equipment would be required to carry out the test method, including power analysers, data loggers and electric vehicle supply equipment (EVSE) testers.

The expertise required of the test engineer would be variable, depending on the assessment option and regulatory requirement under test, but it is recommended that that they have skills both in cyber security and electrical safety.

The Regulations do not mandate compliance with any existing standards and in some cases, there were requirements where no standards could be mapped. However, a review of best practice and standards identified many standards that could be applied which would result in compliance with specific aspects of the regulations. Additionally, assessment options were also developed based on best practice.

The assessment options were validated through a stakeholder workshop and the assessment of two charge point samples that were provided by manufacturers who volunteered to take part in this study. This demonstrated that at least one of five primary assessment strategies could be carried out for each requirement. This also informed minor modifications to the assessment methodology to help streamline the testing.

As detailed in the *Challenges with assessing compliance section*, there may be some difficulties in proving that a charge point is compliant to The Electric Vehicles (Smart Charge Points) Regulations 2021, such as emulation of DSR, unsatisfactory technical files or randomised delay implementations. However, with the various assessment options categories available to the test engineer, it is expected there will always be at least one successful route of assessing compliance.

Now that The Electric Vehicles (Smart Charge Points) Regulations 2021 are fully in force, the assessment options detailed in this project can be implemented as part of a market surveillance program performed by OPSS. This can help ensure that only safe, secure and compliant charge points are being sold in Great Britain.

Appendix 1: EVSCP requirements mapped against applicable standards

Regulation Number	Requirement Title	Subtitle	Mapped Standard
5 - 1	Smart functionality	Charge point must have smart functionality	PAS 1878 Section 7.4 Consumer action OCPP 2.0.1 OCPP 2.0.1: Part 2 – Specification – Section K. SmartCharging ISO 15118-1:2019 Partial mapping – ID V2G1-ED2-22
5 - 2 (a)	Smart functionality	Send and receive information via communications network	PAS 1878 Section 4.1 Energy smart appliance (ESA) OCPP 2.0.1 OCPP 2.0.1: Part 2 – Specification – Section K. SmartCharging ISO 15118-1:2019 Partial mapping – ID V2G1-ED2-22
5 - 2 (b)(i)	Smart functionality	Smart functionality includes changing rate of charge	PAS 1878 Section 3.1.17 energy smart appliance (ESA) OCPP 2.0.1 OCPP 2.0.1: Part 2 – Specification – Section 3 Charging profiles ISO 15118-1:2019 Partial mapping – ID V2G1-ED2-29

Regulation Number	Requirement Title	Subtitle	Mapped Standard
5 - 2 (b)(ii)	Smart functionality	Smart functionality includes changing time when charge occurs	PAS 1878 Section 3.1.17 energy smart appliance (ESA) OCPP 2.0.1 OCPP 2.0.1: Part 2 – Specification – Section 3 Charging profiles ISO 15118-1:2019 ID V2G1-ED2-23
5 - 2 (c)	Smart functionality	Support for DSR services and response DSR services	PAS 1878 Section 3.1.11 demand side response (DSR) PAS 1879 Section 4.5 ESA manufacturers
5 -2 (d)	Smart functionality	User interface support to operate charge point in accordance with these regulations	PAS 1878 Section 4.1 Energy Smart appliance (ESA) Section 5.1.2.4 User interface Section 7.4 Consumer action
6	Electricity supplier interoperability	Smart functionality continues to work after changing electricity supplier	PAS 1878 Section 7.1 General PAS 1879 Section 5.1 Interoperability
7	Loss of communications network access	Device continues to charge when there is no communications network	PAS 1878 Partial mapping - Section 7.9 Loss of communication EN 303 645 Provision 5.9-2 Code of Practice for Consumer IoT Security Requirement 9 – Make systems resilient to outages

Regulation Number	Requirement Title	Subtitle	Mapped Standard
8 - i	Safety	Overriding the default mode of charging during the default charging hours (10 - 3 (a)) must not result in a risk to the health and safety of the user/owner	
8 - ii	Safety	Overriding the provision of demand side response services (10 - 3 (b)) must not result in a risk to the health and safety of the user/owner	
8 - iii	Safety	Overriding the randomised delay (11 - 2 (b)) must not result in a risk to the health and safety of the user/owner	
9 - 1 (a)	Measuring system	Import or Export of electricity can be measured in watt-hours or kilowatt-hours	PAS 1878 Section 5.6 Actual power value or profile provision OCPP 2.0.1 OCPP 2.0.1: Part 2 – Specification – Section 3.50 MeasurandEnumType
9 - 1 (b)	Measuring system	The amount of time of importing or exporting electricity can be measured	PAS 1878 Partial mapping – Section 5.6 Actual power value or profile provision OCPP 2.0.1 OCPP 2.0.1: Part 2 – Specification – Section 3.50 MeasurandEnumType
9 - 2 (a)	Measuring system	9-1 (a) and 9-1(b) can be checked by the owner any occasion device was used within the preceding 12 months	

Regulation Number	Requirement Title	Subtitle	Mapped Standard
9 - 2 (b)	Measuring system	9-1 (a) and 9-1(b) can be checked by the owner for how much the device was used within a month within the 12 preceding months	
9 - 2 (c)	Measuring system	9-1 (a) and 9-1(b) can be checked by the owner for how much the device was used in the the entirety of the preceding 12 month period	
9 - 3(a)	Measuring system	Device must be able to measure import/export of electricity every one second it is in use, in watts or kilowatts	PAS 1878 Section 5.6 Actual power value or profile provision
9 - 3(b)	Measuring system	Measurements must be provided via a communications network	PAS 1878 Section 5.6 Actual power value or profile provision OCPP 2.0.1 OCPP 2.0.1: Part 2 – Specification – Section 3.1 Meter Values
9 - 4(a)	Measuring system	Measurements must be within 10% accuracy	PAS 1878 Section 5.6 Actual power value or profile provision BS EN IEC 61851-22:2002 Partial mapping – Section 5 Standard conditions for operation in service and for installation
9 - 4(b)	Measuring system	Any inaccuracies are not, as a consequence of the design or manufacture, consistent or predictable	PAS 1878 Section 5.6 Actual power value or profile provision

Regulation Number	Requirement Title	Subtitle	Mapped Standard
10 - 1(a)	Off-peak charging	If the charge point is **NOT** sold with a DSR agreement **AND NOT** configured to comply with the requirements of the DSR agreement **AND** details of DSR agreement are **NOT** included in the statement of compliance **THEN**: Device incorporates pre-set default charging hours outside of peak hours (8am to 11am and 4pm to 10pm on weekdays)	
10 -1(b)(i)	Off-peak charging	If the charge point is **NOT** sold with a DSR agreement **AND NOT** configured to comply with the requirements of the DSR agreement **AND** details of DSR agreement are **NOT** included in the statement of compliance **THEN**: Owner is given opportunity to accept the pre-set default charging hours	
10 -1(b)(ii) 10 -1(b)(iii)	Off-peak charging	If the charge point is **NOT** sold with a DSR agreement **AND NOT** configured to comply with the requirements of the DSR agreement **AND** details of DSR agreement are **NOT** included in the statement of compliance **THEN**: Owner is given opportunity to	PAS 1878 Partial mapping – Section 4.5 Remote user interface

Regulation Number	Requirement Title	Subtitle	Mapped Standard
		remove the pre-set default charging hours **OR** set different default charging hours	
10 - 1(c)(i)	Off-peak charging	If the charge point is **NOT** sold with a DSR agreement **AND NOT** configured to comply with the requirements of the DSR agreement **AND** details of DSR agreement are **NOT** included in the statement of compliance **THEN**: Anytime after first use, the owner is able to change or remove the default charging hours if these are in effect	PAS 1878 Partial mapping – Section 4.5 Remote user interface
10 - 1(c)(ii)	Off-peak charging	If the charge point is **NOT** sold with a DSR agreement **AND NOT** configured to comply with the requirements of the DSR agreement **AND** details of DSR agreement are **NOT** included in the statement of compliance **THEN**: Anytime after first use, the owner is able to set default charging hours if none are in effect	
10 - 3(a) 10 - 3(b)	Off-peak charging	Device can charge an EV during default charging hours (if any), save that the owner must be able to override the default mode of	PAS 1878 Partial mapping – Section 5.3.4.2.4 Mode 3: Consumer override

Regulation Number	Requirement Title	Subtitle	Mapped Standard
		charging during the default charging hours, **AND** owner is able to override the provision of DSR services	
11 -1(a) 11 - 1(b)	Randomised delay	The device is capable of operating with a delay of up to 1800 seconds. The delay must be random, and determined to the nearest second. **AND** The maximum duration of the delay can be increased or decreased via a communications network	PAS 1878 Section 5.5.4.5 Calculating Intended Operation in Routine Mode
11 - 2(a)	Randomised delay	At each relevant time, the device will operate with a delay of up to 600 seconds. The delay must be random, and determined to the nearest second.	PAS 1878 Section 5.5.4.5 Calculating Intended Operation in Routine Mode
11 - 2(b)	Randomised delay	The owner can cancel the randomised delay	PAS 1878 Section 5.5.4.5 Calculating Intended Operation in Routine Mode
11 - 3(a)	Randomised delay	Charge point is configured so the delay will not operate when the owner has overridden it	PAS 1878 Section 5.5.4.5 Calculating Intended Operation in Routine Mode
11 - 3(b) 11 - 3(c)	Randomised delay	Charge point is configured so the delay will not operate when: An equivalent random delay has already been applied to the operation of the device in respect of the relevant time (i.e. you can't have more than 1 random delay at a time)	PAS 1878 Section 5.5.4.5 Calculating Intended Operation in Routine Mode

Regulation Number	Requirement Title	Subtitle	Mapped Standard
		OR it is providing response DSR services at the relevant time	
13 - 1	Assurance	Charge point must be sold with an accompanying Statement of Compliance	
13 - 2(a) 13 - 2(b) 13 - 2(c) 13 - 2(d)	Assurance	Statement of Compliance contains: - Model number or type - Statement the charge point meets regulations and that the seller is responsible for meeting them - Name and address of seller - Signed and dated by or on behalf of the seller	
13 - 3 13 - 4 13 - 6(a) 13 - 6(b) 13 - 6(c) 13 - 6(d) 13 - 6(e) 13 - 6f 13 - 6g	Assurance	If requested by the buyer of the charge point, a copy of the technical file must be provided. The technical file must contain: - Design, manufacture and operation of the charge point - General description and copy of the operating manual - Plain English decriptions of the solutions adopted to meet requirements 5 to 11 (after 30th June 2022), and 1 to 10 of schedule 1 (after 30th December 2022)	

Regulation Number	Requirement Title	Subtitle	Mapped Standard
		- Plain English descriptions and explanations on any diagrams or drawings in the documentation - Any test reports that prove compliance to regulations - Details and version of charge point software at time of sale - Charge point to have latest version of software at time of sale	
14	Register of Sales	The seller must keep a register of all sales within the past 10 years	
12 - 1(a) 12 - 1(b)	General Principles	Charge point must be designed, manufactured and configured to provide appropriate protection against the risk of harm to, or disruption of, the electricity system and the charge point	
12 - 1(c)	General Principles	Charge point must be designed, manufactured and configured to provide appropriate protection for the personal data of the owner and end user	
12 - 2(a)	Passwords	The password is unique, or is set by the owner	PAS 1878 Section 6.11 Secure storage area

Regulation Number	Requirement Title	Subtitle	Mapped Standard
			EN 303 645 Provision 5.1-1 Provision 5.1-2 Code of Practice for Consumer IoT Security Requirement 1 – No default passwords OCPP 2.0.1 Partial mapping – OCPP 2.0.1: Part 2 – Specification – Section 2.2.1 BasicAuthPassword
12 - 2(b)	Passwords	The password cannot be reset to a default password	Code of Practice for Consumer IoT Security Requirement 1 – No default passwords
12 - 3 - 1	Software	Device must support secure software updates	PAS 1878 Section 6.10 Software and firmware updates EN 303 645 Provision 5.3-1 Provision 5.3-2 NIST 8259A Software Update – Common Element 1 Code of Practice for Consumer IoT Security Requirement 3 – Keep software updated OCPP 2.0.1 OCPP 2.0.1: Part 2 – Specification – Section L01 – Secure Firmware Update
12 - 3 - 3(a)	Software	Device checks for updates during first setup and periodically thereafter	PAS 1878 Partial mapping – Section 6.14.1.2 Network connectivity Partial mapping – Section 6.14.2.2.1 General requirements EN 303 645 Provision 5.3-5 Code of Practice for Consumer IoT Security Requirement 3 – Keep software updated

Regulation Number	Requirement Title	Subtitle	Mapped Standard
12 - 3 - 3(b)	Software	Device verifies authenticity and intergrity of each software update	PAS 1878 Section 6.10 Software and firmware updates Section 6.14.1.2 Network connectivity EN 303 645 Provision 5.3-9 NIST 8259A Software Update – Common Element 2 OCPP 2.0.1 OCPP 2.0.1: Part 2 – Specification – Section L01 – Secure Firmware Update
12 - 3 - 3(c)	Software	By default, the device notifies the owner about prospective updates	EN 303 645 Provision 5.3-6 Code of Practice for Consumer IoT Security Requirement 3 – Keep software updated
12 - 3 - 3(d)	Software	Software updates are easy to apply	PAS 1878 Section 6.14.2.2.1 General requirements EN 303 645 Provision 5.3-3 NIST 8259A Partial mapping – Software Update – Common Element 6.a Code of Practice for Consumer IoT Security Requirement 3 – Keep software updated
12 - 3 - 4(a)	Software	Using secure boot mechanisms, the software is verified to check it has not been altered other than from an authentic software update	PAS 1878 Section 6.9 Secure boot EN 303 645 Provision 5.7-1 Code of Practice for Consumer IoT Security Requirement 7 – Ensure software integrity

Regulation Number	Requirement Title	Subtitle	Mapped Standard
12 - 3 - 4(b)	Software	if an unauthorised change to the software is detected, it notifies the owner and does not connect to a communications network other than for the purposes of this notification	EN 303 645 Provision 5.7-2 Code of Practice for Consumer IoT Security Requirement 7 – Ensure software integrity
12 - 4 - 1(a)	Sensitive security parameters	Security credentials are protected using robust security measures	EN 303 645 Provision 5.4-1 NIST 8259A Partial mapping – Data Protection – Common Element 1 Code of Practice for Consumer IoT Security Requirement 4 – Securely store credentials and security-sensitive data
12 - 4 - 1(b)	Sensitive security parameters	Software does not use hard-coded security credentials	EN 303 645 Provision 5.4-3 Code of Practice for Consumer IoT Security Requirement 4 – Securely store credentials and security-sensitive data
12 - 5	Secure communication	Communications sent from device must be encrypted	PAS 1878 Section 6.2 Cyber security architecture EN 303 645 Provision 5.5-1 NIST 8259A Data Protection – Common Element 1 Code of Practice for Consumer IoT Security Requirement 5 – Communicate securely OCPP 2.0.1 Partial mapping – OCPP 2.0.1: Part 2 – Specification – Section 1.3.4 TLS with Basic Authentication Profile - 2

Regulation Number	Requirement Title	Subtitle	Mapped Standard
			ISO 15118-1:2019 ID V2G1-ED2-4 ID V2G1-ED2-82
12 - 6 - 1(a) 12 - 6 - 1(b)	Data inputs	Data inputs (UI, API or communications network) are verified so that the type and format of the data is consistent with that expected for the functional to which the data relates If such data cannot be verified, it is discarded or ignored	EN 303 645 Provision 5.13-1 Code of Practice for Consumer IoT Security Requirement 13 – Validate input data
12 - 7 - 1	Ease of use	Setup and operating of the device should minimise inputs from the owner/user	EN 303 645 Provision 5.12-1 Code of Practice for Consumer IoT Security Requirement 12 – Make installation and maintenance of devices easy
12 - 7 - 2	Ease of use	Personal data can be deleted easily	EN 303 645 Provision 5.11-1 Code of Practice for Consumer IoT Security Requirement 11 – Make it easy for consumers to delete personal data
12 - 8 - 1	Protection against attack	There is adequate protection against physical damage to the charge point	BS EN IEC 61851-1:2019 Section 12.11 Mechanical strength – Reference to IEC 62262 IK08 BS EN IEC 61851-22:2002 Section 11.2.2 Mechanical impact – Reference to IEC 60068-2-75

Regulation Number	Requirement Title	Subtitle	Mapped Standard
			EN 62262 Section 4.2 Characteristic group numerals of the IK code and their meanings
12 - 8 - 2	Protection against attack	There must be a tamper-protection boundary to protect internal components	PAS 1878 Section 7.12 Physical protection
12 - 8 - 3(a)	Protection against attack	The device has adequate protection for its user interfaces	
12 - 8 - 3(b)	Protection against attack	The device has adequate protection against use or attempted use of the charge point other than through the user interfaces	
12 - 9(a)	Protection against attack	Any attempt to breach the tamper-protection boundary will notify the owner	PAS 1878 Partial mapping – Section 6.13.1 Event logging and reporting
12 - 9(b)	Protection against attack	Device software runs with minimum level of access privileges required for it to deliver its functionality	EN 303 645 Provision 5.6-7 Code of Practice for Consumer IoT Security Requirement 6 – Minimise exposed attack surfaces
12 - 9(c)	Protection against attack	Unnecessary logical or network interfaces are disabled	PAS 1878 Partial mapping – Section 7.14 Cyber security EN 303 645 Provision 5.6-1 NIST 8259A Partial mapping – Logical Access to Interfaces – Common Element 1

Regulation Number	Requirement Title	Subtitle	Mapped Standard
			Code of Practice for Consumer IoT Security Requirement 6 – Minimise exposed attack surfaces
12 - 9(d)	Protection against attack	Software services are not available to the owner unless necessary for the charge point to operate	EN 303 645 Provision 5.6-5 Code of Practice for Consumer IoT Security Requirement 6 – Minimise exposed attack surfaces
12 - 9(e)	Protection against attack	Any hardware interfaces that are used for the purposes of testing or development, but not otherwise during the operation of the relevant charge point, are not exposed	EN 303 645 Provision 5.6-3 Code of Practice for Consumer IoT Security Requirement 6 – Minimise exposed attack surfaces
12 - 10 - 1 12 - 10 - 2(a) 12 - 10 - 2(b) 12 - 10 - 2(c)	Security Log	The charge point must incorporate a security log that includes any attempts to: - Breach the tamper-protection boundary - Tamper with the device - Gain unauthorised access to the device	PAS 1878 Section 6.11 Secure storage area OCPP 2.0.1 OCPP 2.0.1: Part 2 – Appendices – Section Appendix 1 Security Events
12 - 10 - 3	Security Log	Entries in the security log must record, by reference to Coordinated Universal Time, the time and date on which the event occurred	PAS 1878 Section 6.11 Secure storage area

Regulation Number	Requirement Title	Subtitle	Mapped Standard
12 - 11 - 1 12 - 11 - 2 12 - 11 - 3 12 - 11 - 4(a) 12 - 11 - 4(b)	Provision of information	When the device is sold, information complying with the following requirements must be supplied with it - Contact details with info on how the owner can report concerns or problems regarding the security, including regarding its vulnerability to a cyber attack. - Software update support period - Guidance on how to setup charge point with adequate security - Instructions on how to delete personal data	PAS 1878 Partial mapping – Section 6.13.2 Vulnerability disclosure EN 303 645 Provision 5.2-1 Provision 5.3-13 Provision 5.3-14 (Applicable if device is constrained) Provision 5.12-2 Provision 5.11-3 NIST 8259A Partial mapping – Cybersecurity State Awareness – Common Element 1 Code of Practice for Consumer IoT Security Requirement 2 – Implement a vulnerability disclosure policy Requirement 3 – Keep software updated Requirement 11 – Make it easy for consumers to delete personal data Requirement 12 – Make installation and maintenance of devices easy ISO/IEC 29147 Partial mapping – Section 9.2.2 Preferred contact mechanism

Table 2 – EVSCP Requirements Mapped Against Applicable Standards

Appendix 2: Stakeholder interview topic guide

During the interview process, the stakeholders were asked 20 questions covering topics such as the stakeholders understanding of the regulations, methods of demonstrating compliance, and preferences towards any market surveillance. A list of the questions asked can be seen below:

1. What do you know about the Electric Vehicles (Smart Charge Points) Regulations 2021?
2. Do you know when the Electric Vehicles (Smart Charge Points) Regulations 2021 come into force?
3. What is your understanding of the 'Seller' in the Electric Vehicles (Smart Charge Points) Regulations 2021?
4. As a manufacturer, what do you believe to be your obligations and liability in relation to these regulations?
5. Do you know of any standards that cover the requirements in the Electric Vehicles (Smart Charge Points) Regulations 2021? If so, which standards?
6. Are you aware of any Cybersecurity standards such as EN 303 645?
7. Are you aware if your charge points are compliant to the regulations?
8. If you have any charge points that are not yet compliant, how long do you think it will take to be compliant?
9. What is your approach to achieving compliance to the regulations? E.g. Do you perform any internal testing or assessments?
10. How do you achieve compliance in areas where there are no standards?
11. Which requirements do you believe are the most difficult to be compliant to?
12. How do you plan to demonstrate compliance to the regulations?
13. Do you have a Statement of Compliance (SoC) for any of your charge points?
14. Do you have a Technical file for any of your charge points?
15. If you do not currently have a SoC and/or Technical File, how easy do you think they will be to create and maintain?
16. What would you like to see in a post market surveillance compliance program?
17. Do you foresee any challenges and/or issues arising during any market surveillance?
18. What is your approach to Cybersecurity?
19. Do you perform any Cybersecurity Testing or Audits?
20. Would you like to be involved in a workshop where we can share and discuss our findings on our proposed assessment options?

Appendix 3: Technical file and statement of compliance review checklist

Statement of compliance checklist

This is a recommended checklist to use when assessing compliance. The following table covers the requirements in The Electric Vehicles (Smart Charge Points) Regulations 2021 regarding the seller's statement of compliance (SoC):

Statement of Compliance Requirement	Comments	Status
13-2(a) The model number or type shall be present.		Pending
13-2(a) The model number detailed in the SoC matches the model number present on the charge point.		Pending
13-2(b) The SoC must state that the charge point complies to these regulations and that the seller is responsible for ensuring compliance		Pending
13-2(b) The SoC must state that the seller takes responsibility for ensuring compliance		Pending
13-2(c) The name and address of the seller is present.		Pending
13-2(c) The name and address of the seller matches the company that sold the charge point. The address can be verified by researching the company		Pending
13-2(d) The SoC is signed and dated by the seller, or on behalf of the seller		Pending
13-3 and 13-4 A Technical file is supplied. If a technical file is not already supplied, a technical file was supplied upon request.		Pending

Table 3 – Statement of Compliance Checklist

DSR Agreement Checklist for Regulation 10

Some charge points may be sold with a DSR agreement which will impact the applicability of regulation 10, requirements 10-1(a), 10-1(b)(i), 10-1(b)(ii), 10-1(b)(iii), 10-1(c)(i) and 10-1(c)(ii). If **all** the following points in the below table are met, then the aforementioned requirements are not applicable:

Statement of Compliance Requirement	Comments	Status
The charge point is sold with a DSR agreement		Pending
The charge point is configured to comply with the requirements of the DSR agreement. For example, check to see the charge point has charge schedules setup that comply to what is stated in the DSR agreement		Pending
Details of the DSR agreement are included in the statement of compliance in accordance with the requirements of paragraph 2(b) of regulation 13. Regulation 13 paragraph 2(b) states the SoC must "contains statements that the relevant charge point complies with these Regulations and that the seller is responsible for ensuring that the relevant charge point complies with these Regulations"		Pending

Table 4 – DSR Agreement Checklist

Technical File Checklist

This is a recommended checklist to use when assessing compliance. The following table covers the requirements in The Electric Vehicles (Smart Charge Points) Regulations 2021 regarding the sellers Technical file (TF):

Technical File Requirement	Comments	Status
13-6(a) The design of the charge point is addressed		Pending
13-6(a) The manufacture of the charge point is addressed		Pending
13-6(a) The operation of the charge point is addressed		Pending
13-6(b) A general description of the charge point is present		Pending
13-6(b) The operating manual was supplied		Pending
13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 5		Pending
13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 6		Pending
13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 7		Pending
13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 8		Pending
13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 9		Pending
13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 10		Pending
13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 11		Pending

13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 12-1 Applicable from 30th December 2022		Pending
13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 12-2 Applicable from 30th December 2022		Pending
13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 12-3 Applicable from 30th December 2022		Pending
13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 12-4 Applicable from 30th December 2022		Pending
13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 12-5 Applicable from 30th December 2022		Pending
13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 12-6 Applicable from 30th December 2022		Pending
13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 12-7 Applicable from 30th December 2022		Pending
13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 12-8 Applicable from 30th December 2022		Pending
13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 12-9 Applicable from 30th December 2022		Pending

13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 12-10 Applicable from 30th December 2022		Pending
13-6(c) Written descriptions in plain English of the solutions adopted to meet Regulation 12-11 Applicable from 30th December 2022		Pending
13-6(d) Any diagrams or drawings are accompanied by written descriptions and explanations in plain English		Pending
13-6(e) Copies of any relevant test reports for proving compliance are supplied		Pending
13-6(f) The version of the software on the charge point at the time of sale is present. This version can be verified by checking the software version on the test sample prior to any updates being performed.		Pending
13-6(g) The technical file is up to date at the time of sale		Pending

Table 5 – Technical file checklist

Contact us if you have any enquiries about this publication, including requests for alternative formats, at: OPSS.enquiries@businessandtrade.gov.uk

Office for Product Safety and Standards

Department for Business and Trade,
4th Floor, Multistory, 18 The Priory Queensway, Birmingham B4 6BS
https://www.gov.uk/government/organisations/office-for-product-safety-and-standards