OCPP & UK Electric Vehicles (Smart Charge Points) Regulations 2021

v1.0, 2022-09-28

Table of Contents

OCA Application Note

Relevant for OCPP version: 1.6 and 2.0.1.

Version History

Version	Date	Author	Description
1.0	2022-09-28	Franc Buve *(OCA)*	Final version co-authored by Ashley Grealish *(ev.energy)*, Mathieu Falcy *(Schneider Electric)*, Milan Jansen *(OCA)*

1. Introduction

The number of electric vehicles (EVs) will grow significantly now that UK Government has announced that all new cars and vans must be fully zero emission by 2035. In order to avoid excessive strain on the electricity system, the charging of EVs needs to be managed in such a way that it does not take place during peak-hours and that it can be managed remotely to help balance the grid. Support for this so-called "smart charging" is mandated by the Electric Vehicles (Smart Charge Points) Regulations 2021 for all new private (domestic and workplace) charge points sold in Great Britain. (See [Ref-1]). These regulations have come into force on 30 June 2022, except for the security requirements, which will come into force on 30 December 2022.

In this application note we describe how the smart charging and security capabilities of OCPP can be used to achieve that a charging point [1] meets the requirements of the regulation. The OCPP features that are used for this are supported by:

- OCPP 1.6 with Security Whitepaper
- OCPP 2.0.1 (or higher)

2. Device-level requirements for a charge point

This chapter lists the requirements from [Ref-1] for domestic and workplace charge points and explains how OCPP can be used to fulfill these requirements.

The concept of "demand side response" is often referenced in these requirements. Demand side response (DSR) is the process of adjusting electricity demand to help balance the grid. In case of EVs this is called "smart charging", which is the ability to shift the charging to a time when there is less demand on the grid or when more renewable electricity is available. So-called "response DSR services" refer to instances where charge points are controlled by a third party, e.g. grid operator, to provide a demand response service to the grid ([Ref-2]).

2.1. Smart functionality

A charge point must have smart functionality, which is defined as having the following capabilities in [Ref-1]:

A relevant charge point has smart functionality if:

1. it is able to send and receive information via a communications network;
2. it is able to respond to signals or other information received by it by:
    - increasing or decreasing the rate of electricity flowing through the charge point;
    - changing the time at which electricity flows through the charge point;
3. it is capable of using the functionality referred to in sub-paragraphs (1) and (2) to provide demand side response services, including response DSR services; and
4. at least one user interface, which enables the charge point to be operated in accordance with these Regulations, is incorporated in the charge point or otherwise made available to the owner.

How does OCPP solve this?

Ad 1 Send and receive information

The purpose of OCPP is to support communication between a charge point and a management system.

Ad 2 Respond to signals by changing rate or time of charging

Via OCPP the management system enables smart charging capabilities of the charge point. A management system can submit so-called "charging profiles" to a charge point, which contain a schedule that defines how much power the EV is allowed to draw over a period of time.

Ad 3 Capable of demand side response services

Via the management system the charge point can change this schedule at any time at request of the operator or a third party, for example, when there is a risk of overloading the grid, or to provide response DSR services.

Ad 4 User interface

A user interface of the charge point is a feature that has to be supported by the hardware and firmware of the charge point. This is not directly OCPP-related, although OCPP 2.0.1 does offer support to display information on a charge point. It could also be complied with through the provision of an app, such as our OCA member, ev.energy, are offering.

2.2. Electricity supplier interoperability

This clause has only one requirement in [Ref-1].

1. A charge point must not be configured so that it will cease to have smart functionality if the owner changes their electricity supplier.

The text in [Ref-2] provides a bit more background and states that it is acceptable when a charge point requires reconfiguration when changing electricity supplier, as long as the minimum smart charging capabilities as required by the regulation, are still supported.

Electricity supplier vs. charge point operator

It seems that the regulation refers to the electricity supplier as being the party controlling the charge point. In most market models there are distinct roles for electricity supplier and charge point operator. The electricity supplier is the party that sells the electricity to the charge point owner (i.e. the home or workplace owner). The charge point operator is the party that has the charge point management system to which these charge points are connected and by means of which they are controlled. These roles can in some cases be fulfilled by the same party, though.

Contrary to the situation with public charging points, in the case of home or workplace charge points the charge point operator does not sell the electricity that flows through the charge point. The reason for this is, that the charge point is connected behind the meter of the premise. This means that the charge point is providing electricity that the home or workplace owner has already paid for. Still, even though the charge point operator is technically not supplying the electricity, we assume that the charge point operator performs the electricity supplier role that is mentioned in the regulation.

How does OCPP solve this?

OCPP is an open (i.e. freely available) communications protocol that can be seen as a de facto world-wide standard. This means that it is supported by almost all charge point operators. If the owner changes "electricity supplier" (i.e. charge point operator), then all smart charging capabilities will still be supported when connected to the new party, because they also use OCPP. Since OCPP does not impose any tariff structure, it is not a problem if the new electricity supplier uses an entirely different tariff structure.

2.3. Loss of communications network access

This clause has one requirement in [Ref-1].

1. A charge point must be configured so that, in the event that it ceases to be connected to a communications network, it remains capable of charging an electric vehicle.

How does OCPP solve this?

The above situation — no connection to a communications network — means that the charge point is no longer connected to the charge point management system, because the data connection (cellular, ethernet or Wi-Fi) is down. In OCPP we call this an "offline situation". There are two situations to deal with.

Firstly, in an offline situation it is not possible to request authorization from the management system to start charging, and, secondly, the charge point will not be able to send any usage data to the management system, like the amount of energy consumed. This information should be not be lost, because it may be important to the owner, for example when the energy is reimbursed by the employer for a company car.

There are several ways how offline authorization of charging can be supported by an OCPP charge point.

- The charge point does not require a charge card to start charging and therefore no connectivity is needed to authorize a charge card by the management system.
- The charge point requires a charge card, but the owner’s charge card ID is preconfigured, so it does not require authorization by the management system.
- The charge point requires a charge card, but the charge point has implemented the OCPP authorization cache, so it does not require authorization by the management system, because the charge card is already known from the last time it was used.

When a charging transaction has started in an offline situation, the usage data is automatically stored by the OCPP charge point (this is an OCPP requirement) and will be sent to the management system as soon as the connection is restored.

2.4. Safety

This clause in [Ref-1] requires that any of the following operations shall not result in a risk to the health or safety of persons:

1. overriding the default mode of charging during the default charging hours;
2. overriding the provision of demand side response services;

3. overriding the random delay.

How does OCPP solve this?

The above is about electrical safety of the charge point. This is not in the domain of OCPP and will have to be ensured by the charge point manufacturer.

2.5. Measuring system

[Ref-1] has several requirements related to measurements and storing thereof by the charge point.

1. A charge point must be configured so that on each occasion it is used, it measures or calculates
    - the electricity it has imported or exported (as the case may be), such measurement or calculation to be in watt-hours or kilowatt-hours; and
    - the amount of time for which it is importing or exporting electricity.
2. A charge point must be configured in a way which enables the owner of the charge point to view the information by
    - any occasion on which it was used to import or export electricity within the preceding 12 months;
    - any month within the preceding 12 months;
    - the entirety of the preceding 12 month period.
3. A charge point must be configured so that it can
    - measure or calculate every one second the electrical power it has imported or exported (as the case may be), such measurement or calculation to be in watts or kilowatts; and
    - provide the information via a communications network.
4. A charge point must be configured so that
    - the measured or calculated figures are accurate to within 10% of the actual figure; and
    - any inaccuracies are not systematic.

How does OCPP solve this?

We will address each of the above items separately.

Ad 1 Measuring energy

OCPP records several measurands during a charging transaction. The management system can configure which data to be measured and how often. An OCPP charging transaction always measures the start and end time and register values of the meter. By default, the register value (in Wh) will be sampled during the transaction. (OCPP measurand "Energy.Active.Import.Register"). This is for the regular case of importing electricity.
If the charge point and electric vehicle are capable of delivering energy back to the grid, then the charge point has additional measurands to count the exported energy ("Energy.Active.Export.Register").

Ad 2 Viewing information

The regulation does not specify how the information can be viewed. In theory it can all be stored locally on the charge point and shown on its display (if equipped with one), but since the charge point has sent all recorded data via OCPP to the charge point management system, it is likely that the charge point operator will make this information available to the owner via a website or a mobile app.

Ad 3 Power measurements

A charge point must have the capability to measure imported or exported power every second, and must be able to provide the information via a communications network. The regulation does not specify whether the information has to be sent in real-time or if it can be buffered and sent in larger chunks, but the guide, [Ref-2], suggests that this information is intended to enable response DSR services, in which case real-time transmission can be assumed.
OCPP has configuration variables to specify at which frequency meter values should be sent. The management system can set these intervals to 1 second to support this requirement, whilst providing DSR services, but increase the interval during normal operation.
The OCA member ev.energy has demonstrated the capability to send a power reading every second as an OCPP 1.6 MeterValues.req message when using a 4G or Wi-Fi data connection, so it is technically possible when the data communication channel has sufficient bandwidth.

Ad 4 Accuracy

The accuracy of measurements in the charge point is not related to OCPP. This will have to be ensured by the charge point manufacturer.

2.6. Off-peak charging

A charge point must be configured so that

1. it incorporates pre-set default charging hours which are outside of peak hours;
2. when it is first used, the owner is given the opportunity to
    - accept the pre-set default charging hours;
    - remove the pre-set default charging hours; or
    - set different default charging hours;
3. at any time after it is first used, the owner is able to
    - change or remove the default charging hours if these are in effect;
    - set default charging hours if none are in effect.

The above requirements do not apply where

1. the charge point is sold with a DSR agreement;
2. the charge point is configured to comply with the requirements of the DSR agreement; and
3. details of the DSR agreement are included in the statement of compliance in accordance with the requirements of paragraph (2)(b) of regulation 13 in [Ref-1].

A charge point must be configured

1. to charge a vehicle during the default charging hours (if any), save that the owner of the charge point must be able to override the default mode of charging during the default charging hours; and
2. so that the owner of the charge point is able to override the provision of demand side response services.

Peak hours are defined as 8.00h to 11.00h on weekdays and 16.00h to 22.00h on weekdays.

How does OCPP solve this?

The requirements for off-peak charging can be summarized as follows:

1. the charge point avoids charging during peak hours, or
2. the charge point participates in a DSR agreement, and
3. in both cases the owner can override the schedule or demand side response services.

The following section requires some familiarity with how OCPP charging profiles work. See the side bar OCPP charging profile mechanism for some background.

OCPP charging profile mechanism

A charging profile of type TxDefaultProfile defines a standard schedule for every charging transaction using a list of allowed charging rates over time. The rate is zero when no charging is allowed in that period.
A TxDefaultProfile can be used to define the off-peak charging hours during which charging is allowed. For the peak/off-peak charging schedule it will be configured as a so-called "recurring profile": it has a schedule for a period of 24 hours and then repeats every day. On weekends, however, the off-peak hours do not apply, so another TxDefaultProfile needs to be used on Saturday and Sunday. This is achieved by defining a second TxDefaultProfile for the weekend, that has a schedule of 48 hours with a weekly recurrence. This second TxDefaultProfile has a higher *stack level*, so that it overrules the standard daily occurrence that applies to weekdays.

(1) TxDefaultProfile, stack #1: peak hours from 8.00h to 11.00h and 16.00h to 22.00h.

```
"chargingProfile": {
  "id": 10, "stackLevel": 1, "chargingProfilePurpose":
"TxDefaultProfile",
  "chargingProfileKind": "Recurring", "recurrencyKind": "Daily",
  "chargingSchedule": [ {
    "id": 1, "startSchedule": "2022-06-30T00:00:00",
    "duration": 86400, // 24 hrs
    "chargingRateUnit": "W",
    "chargingSchedulePeriod": [
      { "startPeriod": 0, "limit": 999999 },      // 0:00h
      { "startPeriod": 28800, "limit": 0 },       // 8:00h
      { "startPeriod": 39600, "limit": 999999 },  // 11:00h
      { "startPeriod": 57600, "limit": 0 },       // 16:00h
      { "startPeriod": 79200, "limit": 999999 } ] // 22:00h
  } ]
}
```

(2) TxDefaultProfile, stack #2: overruling Saturdays and Sundays to no limit, recurring every week starting 2022-07-02 (a Saturday).

```
"chargingProfile": {
  "id": 11, "stackLevel": 2, "chargingProfilePurpose":
"TxDefaultProfile",
  "chargingProfileKind": "Recurring", "recurrencyKind": "Weekly",
  "chargingSchedule": [ {
    "id": 1, "startSchedule": "2022-07-02T00:00:00", "duration":
172800, // 48 hrs
    "chargingRateUnit": "W",
    "chargingSchedulePeriod": [ { "startPeriod": 0, "limit": 999999 }
]
  } ]
}
```

Charging during peak hours can be avoided by installing a TxDefaultProfile on the charge point, that exists of a daily recurring 24 hours schedule that sets a power limit of 0 W during the peak hour time slots (8-11h, 16-22h). The TxDefaultProfile must exist as a predefined schedule, that the user can accept at first use of the charge point or change to different default charging hours. The owner must be given the option to change this pre-set schedule at any time. This option can be provided via a website or mobile app of the charge point management system. The regulation states that the owner can freely change the default charging hours or even remove the charging schedule completely.

As an alternative to off-peak charging, the charge point can participate in demand side response services. In such a setup the charge point operator will remotely reduce the charging rate when this is requested by the network operator or third party providing flexibility services. The charge point operator reduces the charging rate or delays the charging by sending a (new) TxProfile for the ongoing charging transaction on the charge point.

Finally, the charge point must offer the possibility to temporarily override the charging schedule or demand side response service when one is in effect. A possible solution for this is to either have an app to control the charge point or have an override button on the charge point itself that, when pressed, removes the TxDefaultProfile (for the default schedule) or the TxProfile (for DSR) for the duration of the charging transaction.

2.7. Randomised delay

The randomised delay is introduced to avoid the risk of a spike or sudden drop in demand, when a large number of charge points start charging or change their rate of charging simultaneously, for example when recovering from a power outage or in response to an external signal such as a time-of-use tariff.

1. A charge point must be configured so that
    - it is capable of operating, at each relevant time, with a delay of up to 1800 seconds, such delay to be of a random duration which is determined, to the nearest second, at each such relevant time; and
    - the maximum duration of the delay can be increased or decreased remotely via a communications network.
2. A charge point must be configured so that
    - at each relevant time it operates with a delay of up to 600 seconds, such delay to be of a random duration which is determined, to the nearest second, at each such relevant time;
    - at each relevant time, the owner of the charge point is able to cancel the delay.
3. A charge point must be configured so that the delay will not operate where
    - the owner, or an end-user of the charge point who is not the owner, has overridden it;
    - an equivalent random delay has already been applied to the operation of the charge point in respect of the relevant time; or
    - it is providing response DSR services at the relevant time.

In this regulation “relevant time” means the point at which, electricity would start flowing through the charge point or the rate of electricity flowing through the charge point would be increased or decreased.

How does OCPP solve this?

The above requirements can be summarized as: "Whenever charging starts or the charging rate changes, a random delay up to 600 seconds shall be applied." Although not explicitly mentioned in the regulation, it must be noted that this only applies to changes to the charging rate that are initiated by the charge point — it cannot be applied when the electric vehicle changes the charging rate, for example when the battery is nearly full. Furthermore, the guide [Ref-2] mentions that the requirement to operate with a randomised delay does not apply when the signal to increase or decrease is coming from an energy management system behind the boundary meter point (e.g. from solar PV, battery storage or a home energy management system).

There are two approaches that can be used to implement the randomised delay. It can be controlled by the charge point itself or by the management system.

Delay controlled by charge point

The first approach is to make this a built-in feature of the charge point firmware. Whenever the user starts charging or the charging rate is about to be changed by the charge point, the firmware will apply the randomised delay before starting the charge or applying the change in charging rate. The maximum length of the randomised delay is defined by a configuration variable. For OCPP 1.6 this is the configuration variable "RandomisedDelay". For OCPP 2.0.1 this is the variable "RandomisedDelay" of the component "SmartChargingCtrlr". It must be configured at 600 seconds for now, but should be capable to support up to 1800 seconds. The value can be set to 0 when the owner overrides the randomised delay, or the charge point is providing response DSR services at the time.

A down-side of this approach is, that this randomised delay is not a standard feature that is present in charging points as of today. It would have to be implemented as a firmware change by the manufacturer. The charge point management system needs to check beforehand whether the charge point supports local randomization by requesting the value of the configuration variable "RandomisedDelay". Existence of this variable tells the management system that the charge point performs randomisation locally. If it does not exist, then randomised delay must be taken care of by the management system..

Delay controlled by management system

The second approach is a generic solution that makes the charge point management system responsible for the randomised delay. The section assumes some familiarity with how OCPP charging profiles work. See the sidebar on OCPP charging profile mechanism in Off-peak charging for more information.

The charge point management system has already set a recurring TxDefaultProfile charging profile (if it is not participating in a DSR agreement) that defines the off-peak charging hours. See Off-peak charging. The randomised delay is added to the starting times of the off-peak charging periods (11h-16h,22h-8h) in the TxDefaultProfile, so that not all charge points start charging at the same time (11.00h or 22.00h). This means, for example, that for one charge point the off-peak charging period on a certain day will start at 11:01h and for the next charge point it may start at 11:04h.

This works fine when an electric vehicle connects during peak hours and thus has to wait until off-peak hours before charging can start. This does not work when the electric vehicle connects during the off-peak hours, because then it would start charging immediately.

To avoid this, the charge point management system submits a new TxDefaultProfile with a higher stack level (e.g.

3) than the TxDefaultProfiles that implement the default charging hours. The new TxDefaultProfile is a relative charging profile (i.e. it starts when the transaction starts) and has one period of random length (up to 600 s) with zero power, after which the charging profile ends and the charge point falls back to the TxDefaultProfiles that implement the default charging hours.

Since every charging session should have a different randomised delay, the charge point management system will submit a new TxDefaultProfile (with a new randomised delay) to be used for the next session when the current charging session ends.

NOTE	Not all electric vehicles may respond kindly to receiving zero power when starting a transaction. Some might interpret this as an error situation. It is up to the charge point manufacturer and the charge point management system to design how to work around these limitations.

2.8. Security

The following requirements about security are laid out in [Ref-1]. The security requirements will come into force on 30 December 2022. The numbering of these subsections matches the paragraphs numbers in the regulation.

2.8.1. General principles

A charge point must be designed, manufactured and configured to provide appropriate protection

- against the risk of harm to, or disruption of, the electricity system;
- against the risk of harm to, or disruption of, the charge point;
- for the personal data of the owner and any other end-user of the charge point.

How does OCPP solve this?

These subjects are not in the realm of OCPP. They need to be addressed by the charge point manufacturer.

2.8.2. Passwords

A charge point must be configured so that where passwords are used on it

- the password is unique to that charge point and not derived from, or based on, publicly-available information, or is set by the owner; and
- the password cannot be reset to a default password applying to both that charge point and other charge points.

How does OCPP solve this?

OCPP requires that the basic authentication password of a charge point must consist of a randomly chosen string of at least 16 and at most 40 characters.

- For OCPP 2.0.1, requirements A00.FR.205, A00.FR.304. [Ref-3]
- For OCPP 1.6, requirements A00.FR.205, A00.FR.304. [Ref-4]

2.8.3. Software

1. A charge point must incorporate software which is able to be securely updated.
2. In sub-paragraph (1), securely updated means updated using adequate cryptographic measures to protect against a cyber-attack.
3. A charge point must be configured so that
    - it checks, when it is first set up by the owner, and periodically thereafter, whether there are security updates available for it;
    - it verifies the authenticity and integrity of each prospective software update by reference to both the data's origin and its contents and only applies the update if the authenticity and integrity of the software have been validated;
    - by default, it provides notifications to the owner about prospective software updates;
    - the owner can implement software updates without undue difficulty.
4. A charge point must be configured so that
    - it verifies, via secure boot mechanisms, that its software has not been altered other than in accordance with a software update which has been validated in accordance with subparagraph (3)(b) above;
    - 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.

How does OCPP solve this?

In OCPP the firmware updates are controlled by the charge point management system, which will notify a charge point whenever a firmware update is available.

OCPP provides a secure firmware update mechanism that requires that a signing certificate from the manufacturer, which the charge point will use to check the integrity of the firmware image. This process is described in:

- OCPP 2.0.1, use case L01 in section "L. FirmwareManagement" of [Ref-3].
- OCPP 1.6, use case L01 in section "4. Secure Firmware Update" of [Ref-4].

2.8.4. Sensitive security parameters

1. A charge point must be configured so that
    - where security credentials are stored on the charge point, these are protected using robust security measures;
    - its software does not use hard-coded security credentials.
2. In this paragraph
    - "hard-coded" means data forming part of the charge point's source code and which is unalterable except by means of modification of the source code;

- “security credentials” means ways of verifying that the charge point is being used or accessed by a person properly authorised to do so.

How does OCPP solve this?

These subjects are not in the realm of OCPP. They need to be addressed by the charge point manufacturer.

2.8.5. Secure communication

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

How does OCPP solve this?

OCPP 1.6 and 2.0.1 define three levels of security:

- Security profile #1: Unsecured transport with basic authentication
- Security profile #2: TLS with basic authentication
- Security profile #3: TLS with client side authentication

OCPP recommends to use security profile #2 or #3, both of which use TLS (Transport Layer Security), which provides encrypted communication.

2.8.6. Data inputs

1. A charge point must be configured so that
    - data inputs are verified so that the type and format of the data is consistent with that expected for the function to which the data relates;
    - if such data cannot be verified, it is discarded or ignored by the charge point in a safe manner.
2. The data inputs referred to in sub-paragraph (1) include data that is inputted via a user interface, an application programming interface or a communications network.

How does OCPP solve this?

The format of all OCPP messages is defined in the OCPP JSON schemas. Messages that do not comply with the JSON schema will not be accepted by a compliant charge point or management system.

2.8.7. Ease of use

1. A charge point must be configured so as to minimise the inputs required from the owner in connection with the set-up and operation of the charge point.
2. A charge point must be configured so that any personal data can be deleted from it by the owner without undue difficulty.

How does OCPP solve this?

OCPP has no effect on the user interface for the owner in relation to set-up and operation.

OCPP 2.0.1 does define a specific operation to clear personal information: Use case N01 "Clear Customer Information" in section "N. Diagnostics" of [Ref-3].

2.8.8. Protection against attack (1)

1. A charge point must be designed and manufactured to provide an adequate level of protection against physical damage to the charge point.
2. In particular, a charge point must incorporate a tamper-protection boundary to protect the internal components of the charge point.
3. A charge point must be designed and manufactured to provide an adequate level of protection
    - for its user interfaces; and
    - against use or attempted use of the charge point other than through the user interfaces.

How does OCPP solve this?

These subjects are not in the realm of OCPP.

2.8.9. Protection against attack (2)

A charge point must be configured so that

- if there is an attempt (whether or not successful) to breach the tamper-protection boundary, it notifies the owner;
- its software runs with only the minimum level of access privileges required for it to deliver its functionality;
- any logical or network interfaces that are not required for the normal operation of the charge point, or otherwise to comply with the requirements in these Regulations, are disabled;
- software services are not available to the owner unless necessary for the charge point to operate;
- any hardware interfaces that are used for the purposes of testing or development, but not otherwise during the operation of the charge point, are not exposed.

How does OCPP solve this?

Most of the above subjects are related to the firmware development of the charge point in general. For item 1, notification in case of tampering, OCPP 2.0.1 offers a security event notification, as described in use case A04 "Security Event Notification" of section "A. Security" in [Ref-3]. The same mechanism exists for OCPP 1.6 in use case A04 of section "3. Security events/logging" of [Ref-4].

2.8.10. Security log

1. A charge point must incorporate a security log.
2. In this paragraph, “security log” means an electronic record on the charge point of events relevant to the security of the charge point including attempts (whether or not successful) to
    - breach the tamper-protection boundary;

- tamper with the charge point; or
- gain unauthorised access to the charge point.

3. Entries in the security log must record, by reference to Coordinated Universal Time, the time and date on which the event occurred.

How does OCPP solve this?

OCPP defines security events that need to be logged in a security log. Critical events also need to be reported immediately to the management system. Examples of these are: TamperDetectionActivated, SecurityLogWasCleared and FirmwareUpdated. The management system can request the charge point via OCPP to upload the log to the server, when necessary.

2.8.11. Provision of information

1. When a charge point is sold, information complying with the requirements in sub-paragraphs (2) to (4) must be supplied with it.
2. The information must specify how the owner can report concerns or problems identified regarding the security of the charge point, including regarding its vulnerability to a cyberattack. In particular, the information must provide contact details to which such concerns or problems can be reported.
3. The information must specify the period, if any, for which software updates will be provided by or on behalf of the charge point manufacturer.
4. The information must
    - provide guidance on how to set up the charge point with adequate security protection;
    - include instructions on how to delete personal data from the charge point.

How does OCPP solve this?

These subjects are not in the realm of OCPP.

2.9. Assurance

The requirements with respect to assurance do not relate to OCPP, and are therefore skipped in this document.

2.10. Register of sales

The requirements with respect to a register of sales do not relate to OCPP, and are therefore skipped in this document.

3. References

(1) 2021 No. 1467, ROAD TRAFFIC, The Electric Vehicles (Smart Charge Points) Regulations 2021, https://www.legislation.gov.uk/

(2) Complying with the Electric Vehicles (Smart Charge Points) Regulations 2021,
Guidance for sellers of electric vehicle charge points in Great Britain, May 2022,

(3) OCPP 2.0.1 Part 2 - Specification, Open Charge Alliance, 2020-03-31.

(4) Improved security for OCPP 1.6-J edition 3, Open Charge Alliance, 2022-02-17

[1] Charge point and charging station are synonymous. "Charge point" is the formal name in OCPP 1.6, whereas "charging station" is used in OCPP 2.0.1.