VCHRGD SEVEN Technical File

The Electric Vehicles (Smart Charge Points) Regulations 2021

Charge point make:	VCHRGD TECHNOLOGIES LTD
Charge point model:	VCHRGD SEVEN TETHERED (E007STH-01) VCHRGD SEVEN UNTETHERED (E007SUH-01)
Software version at point of sale:	2.0.4
Seller: *Person responsible for compliance with the Regulations*	VCHRGD TECHNOLOGIES LTD
Manufacturer(s): *If different to seller*	VCHRGD TECHNOLOGIES LTD
Last update to technical file:	01/01/2026

The VCHRGD Seven is a compact and cost effective solution for smart EV charging The charger is a

single phase, 32 A 7 kW) charger, but can be limited to a current from 6 A up to 32 A.

It's understated, stylish and compact design is in harmony with its simple operation installation, coming in a sleek matte black finish.

Available in tethered complete with a 5 m length cable and European Standard Type 2 connector, or untethered with a universal Type 2 Socket it's an ideal choice for domestic charging.

Integral PEN protection, means that no additional earth rod is required, and simple connections make the installation process fast and efficient. WiFi Bluetooth Connectivity allow for remote authorisation, charge scheduling and diagnostics via mobile app and online portal.

Operating manual

Copy of operating manual as available at point of sale can be found *(cross as appropriate)***:**		~~Attached to this document (hard copy)~~
		~~Attached to this document as a digital file (soft copy)~~
		Available online via hyperlink (soft copy)
Link if available online:	VCHRGD SEVEN Operations Manuals Sharepoint	

Version of file received at point of sale if available online:	V2.0

VCHRGD TECHNOLOGIES LTD 2023

Technical solutions implemented to meet the requirements of the Regulations

Smart functionality

Requirement	Technical solution adopted to meet the requirement
Charge point is able to send and receive information via a communications network	Chargepoint sends and receives information via WiFi connected to users router. (IEEE 802.11bgn) @2.4Ghz WPA-2
Charge point 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	The charge point is capable of increasing and decreasing the rate of electricity flowing through it by adjusting the output current between 0A and 32A. The charge point is capable of adhering to a smart charging schedule, regulating the output depending on a customers desired charge level, start and stop times, and integrating required delays and pre-set schedules. All controlled via the connected back-end and user app.
Charge point is capable of using this functionality to provide demand side response services, including response DSR services	The charger can provide DSR response via back-end API integration if required, we are actively working on linking to DSR providers to offer DSR services to customers.
Charge point has at least one user interface, incorporated in the charge point or otherwise made available to the owner	The charge point has 3 user interfaces: Mobile App Control RFID Emergency Start/Stop button

Electricity supplier interoperability

Requirement	Technical solution adopted to meet the requirement
Charge point is configured such that is will not cease to have smart functionality if the owner changes their electricity supplier	The charge point operation is not restricted by the end user electricity supplier, and any DSR service integrations will be dynamic and easily switchable to ensure no limiting of functionality.

Loss of communications network access

Requirement	Technical solution adopted to meet the requirement
Charge point is configured such that, in the event it ceases to be connected to a communications network, it will remain capable of charging an electric vehicle	If the charge point ceases to be connected to the back-end due to a WiFi drop-out or loss of service, the charger will continue to operate. If connection is lost prior to a charge session being started then the user can utilise the RFID cards or plug & charge to begin a session. If the connection is lost during an active charging session, the charger will continue to follow the pre-set schedule and report meter reading and session status when it reconnects.

Safety

Requirement	Technical solution adopted to meet the requirement
Charge point is configured such that it will not allow a relevant person to carry out a specified operation where to do so would or may result in a risk to the health or safety of persons. "Relevant persons" means the owner, or an end-user of the relevant charge point who is not the owner. "Specified operation" means: • Overriding the default mode of charging during the default charging hours • Overriding the provision of demand side response services • Overriding the random delay	The intrinsic safety features of the charger, such as the earth leakage monitoring, over voltage and over current conditions are not configurable or editable by the end-user or owner. The charger is configured such that no operation, including: • Overriding the default mode of charging during the default charging hours • Overriding the provision of demand side response services • Overriding the random delay Would or may result in a risk to the health or safety of persons.

Measuring system

Requirement	Technical solution adopted to meet the requirement
On each occasion it is used, the charge point measures or calculates: • The electricity it has imported or exported (in watt-hours or kilowatt-hours) • The amount of time for which it is importing or exporting electricity	The charger utilises on board current monitoring and an internal clock, as well as back-end clock-aligned consumption periods to calculate the electricity it has exported, this is then used to calculate and report the exported values in watt-hours to the charger and back-end. These values are reported as: • Energy.Active.Import.Register – unit watt-hours (wH) • Power.Active.Import – unit Watts (W)

	• Current.Offered – Unit Amps (A)
The charge point is configured such that the owner can view the information in reference to: • Any occasion on which it was used to import or export electricity within the past 12 months • Any month within the past 12 months • The entirety of the last 12-month period	The charge point back-end is configured to report charging statistics and session history, including: • This month • Last Month • All Time • Custom Time Period configurable by user between 2 dates This information is readily accessible to the user via the mobile application.
The charge point is configured such that it can: • On each occasion it is used, measure or calculate every one second the electrical power it has imported or exported (in watts or kilowatts) • Provide this information via a communications network	The charge point is configured to report meter values at configurable intervals, historically this has been reported every 60s to the user via the mobile app and to the back-end via WiFi connection. 60s was chosen to minimise bandwidth consumption and simplify back-end diagnostics. The meter value duty cycle from June 30th will be configured to report every 1s.
The charge point is configured such that: • The figures measured or calculated are accurate to within 10% of the actual figure • Any inaccuracies are not systematic	The calculated import and export figures measured and calculated via the charger are configured such that they are accurate to within ±0.5% as defined by the maximum permissible limit of error for the current transformer used to measure exported current internally.

Off-peak charging

Requirement	Technical solution adopted to meet the requirement
The charge point: • Has pre-set default charging hours which are outside of peak hours • Offers the owner the opportunity to accept, remove, or change the default charging hours on first use • Offers the owner the ability to change, remove, or set default charging hours any time after first use unless the charge point is sold with a DSR agreement, configured to comply with the requirements of this agreement, and details of the	The charge point: • Has pre-set default charging hours which are outside of peak hours - Peak hours defined as 8:00 - 11:00AM - 16:00 - 22:00PM on weekdays The VCHRGD Seven pre-configured default charging hours are set to 22:00PM – 07:00AM The charge point is pre-configured with a default charging schedule outside of peak hours. This charger is set on the charge point and is applied even when the charger is offline. The charge point is also configured to connect to the CPMS given it is connected to the Internet.

agreement are included in the statement of compliance	The owner downloads the mobile app and after the initial setup of the charger, the app presents the option to the owner to view and accept the default charging schedule (off-peak hours), to set their own schedule, or to remove the charging schedule. Any change of the schedule by the owner in the mobile app is communicated to the charge point and stored locally on the charge point, so even if it goes offline, the schedule will still apply. The way the schedule is communicated to the charger is via the Internet via OCPP. This is how it works: 1. The charging schedule (default or set by the owner) is communicated to the charger (TxDefaultProfile) at first use or at any change made by the owner; 2. When the charger is connected, the charging schedule is applied by the CPMS (TxProfile) at the start of a charging session; 3. When the charger is offline, the charger follows the last known schedule.
The charge point is configured: • To charge a vehicle during the default charging hours (if any), unless the owner overrides the default mode of charging during this time • Such that the owner can override the provision of demand side response services	The charge point charges the vehicle based on the set charging schedule. Unless changed or removed by the owner, the default charging schedule applies. Using the mobile app the owner can override the schedule during a charging session, for the current charging session - for example if they need the car charged sooner, and is an isolated override to that specific session. The owner can also change the charging schedule by manually selecting the hours during which they want to charge their vehicle. In the mobile app, the owner can use a “boost” option during a running charging session to override the current schedule or DSR settings for this current charging session. Using the “boost” does not affect the recurring schedule of the charge point but only the current charging session.

Randomised delay

Requirement	Technical solution adopted to meet the requirement
The charge point is configured such that it must operate, at each relevant time, with a delay of random duration up to 600 seconds, determined to the nearest second each time	The charge point is applying a randomised delay in all of the following use-cases: 1. On charging start without schedule (when online - it is done by the CPMS) 2. On power increase/decrease based on user-defined charging schedule or the default off-peak schedule set by the manufacturer.

	For example, the owner has set the start time for 11 pm, the charger applies a delay of up to 10 min and starts charging, for example at 11:04 pm; --- this is applied by the CPMS and the charger receives the schedule with the delay calculated in it. 1. When charging **offline** - at the start of a session and on power increase/decrease due to schedule Randomised delay is not applied in the following cases: 1. When applying a schedule based on a TOU tariff (Agile Octopus, Octopus Go); --- as these are treated as DSR agreements 2. When decreasing/increasing power due to the use of DLM; A delay of random duration is applied anytime the charger starts or resumes charging or the power is increased or decreased. The maximum delay interval can be set in the CPMS backend (default is 600 seconds). The delay is randomly applied for each event where the charging starts, resumes or the power is increased or decreased. This is applied and managed by the CPMS, which sends the charging schedule to the charge point via OCPP, with the delay calculated in the schedule sent to the charger. Any change of the random delay duration in the CPMS is communicated to the charge by the means of a configuration key change (via OCPP) that controls the duration of the random delay.
The charge point is configured such that the maximum duration of this delay can be remotely increased to up to 1800 seconds if required	The charger can be reconfigured remotely to increase the max randomised delay to up to 1800 seconds. This is done via OCPP by changing the value of a specific configuration key. The default maximum duration of the delay can be adjusted in the CPMS backend, and the change is communicated to the charger with an OCPP command to change the specific configuration key that controls the random delay duration.
The charge point is configured such that the random delay will not operate where: • The owner or another relevant end-user has manually overridden it • An equivalent random delay has already been applied to the operation of the relevant charge point	A randomised delay is not applied in the following cases: • The owner uses the Boost function in the app during a charging session • The owner edits the charging schedule during a charging session • A flexible electricity tariff is used to determine the charging schedule

• The charge point is responding to a response DSR service	• Power is increased/decreased by Dynamic Load Management (local, or cloud)

Security

[Information in this section is only required from 30 December 2022. Before this date, completing this section is optional.]

Requirement	Technical solution adopted to meet the requirement
General principles The charge point is 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 relevant charge point	The CE certification of the charge point can effectively protect the charge point and electricity system; The owner's personal data is not stored in the charge point. The backend and APP should also ensure the security of personal data.
Passwords The charge point is configured such that where passwords are used on it: • The password is unique to the charge point and not derived from, or based on, publicly available information, or is set by the owner • The password cannot be reset to a default password applying to both the charge point and other charge points	(1) A local interface for offline configurations It is accessed via a browser by connecting to the charge point via bluetooth. The access is protected with a password, which is unique for the charge point and is not derived from, or based on, publicly available information. This password can be changed by the installer and recovered using algorithmically generated key word, where the default password is unique for the charge point and only applies to this specific charge point. (2) Mobile app The owner sets their own password upon registration. There is no default password for the mobile app, it is set by the owner. The owner can set a new password if needed by providing the old one or by using e-mail verification if the old password is lost or forgotten. There is no option to reset the password to a default one.
Software The charge point incorporates software which is able to be securely updated using adequate cryptographic measures to protect against cyber attack	Firmware updates are provided OTA via secure https firmware repository and all charger firmware is verified for download.

Software The charge point is configured such that: • It checks for security updates available when first set up by the owner and periodically after • It verified 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	When first set up by the owner, the charger checks for firmware updates and if one is available, the owner is presented with the option to update the firmware. Then, at every connection to the CPMS (including after each reboot or power cycle), a check for new firmware update is performed and if one is available, it is applied automatically. The owner receives a push notification when a firmware update has been applied. The owner also has the option to check the firmware version and check for updates in the mobile app and if one is available – to apply it. Updates are applied "over the air" and do not require any technical or specific knowledge from the owner. The CPMS allows for firmware updates to be applied even without any owner interaction being required (the owner is still notified).
Software The charge point is configured such that: • It verifies via secure boot mechanisms that its software has not been altered other than in accordance with a validated software update • If unauthorised change to software is detected, it notifies the owner and does not connect to a communications network other than for purposes of this notification	It is necessary to verify the integrity of the firmware every time the Boot is started. If it is modified, it will be prompted by a flashing red indicator light and the event will be recorded. If an unverified firmware update is attempted, the charger will remain in a fault condition until power cycled, at which point the unit will return to an operational condition under the previously bootloaded firmware version.
Sensitive security parameters The charge point is configured such that: • Security credentials stored on the charge point are protected using robust security measures • Software does not use hard-coded security credentials	Passwords and CA certificate are stored using AES encryption.
Secure communication The charge point is configured such that communications it sends are encrypted	Communication between the charger and CPMS is encrypted. OCPP communication supported by TLS1.2 Local BLE connection secured using AES encryption
Data inputs	Data inputs in the app such as power limit, charging schedule, etc. are possible only within pre-defined safe

The charge point is configured such that: • Data inputs are verified so that the type and format of the data is consistent with that expected for the function • If such data cannot be verified, it is discarded or ignored by the charge point in a relevant manner	options and format. Additionally, all data inputs are verified by the CPMS before being submitted to the charger. The charger would then verify any commands and data inputs received from the CPMS and will discard ones that cannot be verified – either for invalid format, type or if outside safe parameters.
Ease of use The charge point is configured to minimise the inputs required from the owner in connection with its set-up and operation	Owner only needs to "claim" the charge point by entering the ID & PIN that comes with the charger. Nothing else is really needed unless the owner wants to change any of the default settings, which is entirely optional and easy to do in the app. The setup of the charger by the owner requires minimum input. The owner uses the mobile app and follows a streamlined setup wizard to connect the charger. Upon initial connection, the charger is pre-configured with scheduled charging and while the owner can change the schedule and other settings on the charger, no additional inputs are required to start using the charger or to operate it in general.
Ease of use The charge point is configured such that any personal data can be deleted from it by the owner without undue difficulty	Personal data stored in the CPMS can be deleted by the owner directly, in the app account menu.
Protection against attack The charge point is designed and manufactured to provide an adequate level of protection against physical damage to the charge point	We added a micro switch to the cover of the charge point. Once the charge point is disassembled, the charge point will detect the signal that the micro switch is disconnected, and the charge point will judge it as a tamper event, record and send it to backend, backend then notify the owner through the APP.
Protection against attack The charge point incorporates a tamper-protection boundary to protect the internal components of the charge point	The charge point does not provide other communication interfaces except the APP UI for human access, which can effectively protect the charge point from unknown access. When an attempt to breach the tamper protection is detected, the charger notifies the CPMS and the owner receives a notification on their phone.
Protection against attack The charge point is designed and manufactured to provide an adequate level of protection to its user interfaces and against use or attempted use of the charge point other than through the user interface	The chargepoint front plate and wiring access are protected by security screws and a tamper detection switch which generates a fault condition, limits charging and notifies the end user via OCPP to the tamper event and timestamps the event. Additional tamper tape has been applied to one of the rear access screw points.

Protection against attack The charge point is configured such that: • If there is an attempt to breach the tamper-protection boundary, the owner is notified • Its software runs with only the minimum level of access privileges required to deliver functionality • Any logical or network interfaces that are not required for the normal operation of the charge point or otherwise comply with the Regulations are disabled • Software services are not available to the owner unless necessary for the relevant 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	When an attempt to breach the tamper protection is detected, the charger notifies the CPMS and the owner receives a notification on their phone.
Security log The charge point incorporates a security log – an electronic record which includes attempts (whether or not successful) to: • Breach the tamper-protection boundary • Tamper with the relevant charge point • Gain unauthorised access to the charge point These entries must record the time and date the event occurred (by reference to Coordinated Universal Time).	All security events detected by the charge point or by the CPMS are logged. A security log is maintained for the charger, which includes tamper-protection breaches, unauthorized access attempts, and software tamper attempts. The security events log is available to the owner in the mobile app. All entries in the log contain a timestamp (shown to the owner in the local time zone, stored in the system in UTC), the type of the event, and additional information.

Test reports

Name of test	Date of test	Outcome	Certificate attached to file?	Notes (e.g., did test occur via third party?)
Smart functionality test: send and receive communications	FEB-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE
Smart functionality test: increase and decrease charging rate	FEB-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE
Smart functionality test: change time of electricity flow	FEB-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE
Loss of communications network access	MARCH-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE
Safety	JAN-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE
Measuring System: Exported energy and time	JAN-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE
Measuring System: Charging history	MARCH-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE
Measuring System: 1 second export	MAY-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE
Off Peak Charging: Pre-set schedule with charger on commissioning	MAY-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE
Off Peak Charging: Opt out, schedule configure and	JUNE-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE

boost charge function				
Randomised Delay: Charger ability to apply delay of (n) seconds provided n ≤600s to scheduled sessions	JUNE-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE
Randomised Delay: Charger ability to apply delay of (n) seconds provided n ≤1800s to scheduled sessions	JUNE-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE
The charge point is configured such that where passwords are used on it: The password is unique to the charge point and not derived from, or based on, publicly available information, or is set by the owner The password cannot be reset to a default password applying to both the charge point and other charge points	DEC-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE
The charge point incorporates software which is able to be securely updated using	DEC-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE

adequate cryptographic measures to protect against cyber attack				
It checks for security updates available when first set up by the owner and periodically after It verified 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	DEC-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE
The charge point is configured such that: It verifies via secure boot mechanisms that its software has not been altered other than in accordance with	DEC-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE

a validated software update If unauthorised change to software is detected, it notifies the owner and does not connect to a communications network other than for purposes of this notification				
The charge point is configured such that: Security credentials stored on the charge point are protected using robust security measures Software does not use hard-coded security credentials	DEC-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE
The charge point is configured such that: Data inputs are verified so that the type and format of the data is consistent with that expected for the function If such data cannot be verified, it is discarded or ignored by the charge point in a relevant manner	DEC-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE

The charge point is designed and manufactured to provide an adequate level of protection against physical damage to the charge point	DEC-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE
The charge point incorporates a tamper-protection boundary to protect the internal components of the charge point	DEC-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE
The charge point is designed and manufactured to provide an adequate level of protection to its user interfaces and against use or attempted use of the charge point other than through the user interface	DEC-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE
The charge point is configured such that: If there is an attempt to breach the tamper-protection boundary, the owner is notified Its software runs with only the minimum level of access privileges required to	DEC-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE

deliver functionality Any logical or network interfaces that are not required for the normal operation of the charge point or otherwise comply with the Regulations are disabled Software services are not available to the owner unless necessary for the relevant 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				
The charge point incorporates a security log – an electronic record which includes attempts (whether or not successful) to: Breach the tamper-protection boundary Tamper with the relevant charge point Gain unauthorised	DEC-2022	PASSED	NO	TESTS CONDUCTED IN HOUSE

access to the charge point These entries must record the time and date the event occurred (by reference to Coordinated Universal Time).				