

Solo 3

Technical File

The Electric Vehicles (Smart Charge Points)
Regulations 2021

This document is the technical file for the following chargepoint:

Chargepoint make:	Pod Point
Chargepoint model:	Solo 3: S7-UC-03, S7-UCB-03, S7-2C-03, S7-1C-03, S22-UC-03, S22-2C-03
Compliant software versions:	Refer to the Pod Point App to see the current software version running on your charger A30P-5.0.0
Seller:	Pod Point Ltd. 28-42 Banner Street, London, EC1Y 8QE
Last update to technical file:	14th Dec 2022



Solo 3
Universal



Solo 3
Tethered

Description of the smart charge point

The Solo 3 includes and exceeds all required and “optional” safety features noted in the BS EN 61851-1 standard for electric vehicle charging. The Solo 3 is available in a universal socketed or tethered model, with either Type 1 or Type 2 cables. The Solo 3 is available in charging rates of either 3.6kW, 7kW or 22kW. The auto power balancing feature is not available on the 22kW model.

The Solo 3 incorporates a simple LED user interface on the charger itself, with more advanced operations available via the Pod Point App. A Wi-Fi connection for the charger is required for app functionality.

User Guide

A copy of the operating instructions for this charger can be found at:
pod-point.com/solo-3-user-guide

The following technical solutions have been implemented to meet the requirements of the regulations when a charger is installed in a domestic setting.

Smart functionality

The Solo 3 is able to connect to a communications network via a local Wi-Fi network, or where installed, a cellular data link.

The Solo 3 can respond to commands sent over the communication network to alter the allowed current limit during a charge, including pausing the charge. This mechanism allows the Solo 3 to participate in DSR services and scheduled or 'off-peak' charging.

The LED on the front of the Solo 3 indicates its current status and users are able to schedule their charges via the Pod Point App.

Electricity supplier interoperability

The Solo 3 is not dependent on any particular electricity tariff or provider and will continue to provide all functions on any suitable power supply, including features available via the Pod Point App.

Loss of communications network access

In the event that the Solo 3 is unable to connect to the communication network, it will default to charging the vehicle when plugged-in, subject to an (up to) 600 second random delay in some circumstances. For example:

- the random delay is applied if a Solo 3 is energised when a vehicle is already plugged-in.
- if the communication network becomes unavailable during a paused charging session.

To ensure the owner remains in direct control, the time schedule will be ignored while the communication network is unavailable and a plugged-in vehicle will charge subject to the random delay.

Safety

Local safety systems within the Solo 3 will take priority over commands to start charging received via the communication network or the user overriding random delays, demand side response actions or default schedule settings. These are designed to prevent overloading of the circuit supplying the charger and mitigate against the risk of electric shock.

Measuring system

The Solo 3 is capable of measuring:

- Electricity flowing to a connected vehicle, in kilowatt-hours (kWh).
- The total time within a charging session during which power was flowing.

This information is available via the Pod Point App. The app can be used to view all charges within the last 12 months. These can be viewed individually, or grouped by week, month or year.

Solo 3 electrical power measurements sent over the communication network have been tested to be accurate within 10%. The electrical power measurements are made every 1 second. Power measurements will not be sent during periods of unavailability of the communication network. Therefore, unavailability of the communication network from time to time may lead to some inaccuracy in monthly or annual aggregated charge statistics.

Off-peak charging

After completion of an installation and once the charger has been connected to the Pod Point App, the Solo 3 will have a default schedule activated to charge vehicles when demand on the electricity grid is lowest.

You can change the schedule times or disable the scheduling feature via the Pod Point App.

If the charger is sold with a DSR agreement, allowing a third party to manage the charging rate and control energy usage for a defined group of chargers, the schedule will not be activated.

Randomised delay

During the following scenarios, a random delay of up to 600s will be applied to a charge's start or stop operation:

1. When a charge is started or stopped by a user created schedule or the default charging schedule.
2. When the Solo 3 is energised and it is already connected to a vehicle which is able to accept charge.
3. When the communication network becomes available and the Solo 3 is set to perform a scheduled charge.
4. When the communication network becomes unavailable outside of the user's scheduled charging times and a vehicle which is able to accept charge is connected.

The duration of the random delay is capable of being increased to 1800 seconds if required.

A user can override this delay in each case by either temporarily disabling the schedule (in scenario 1) or by unplugging the vehicle and reconnecting it (in scenarios 2, 3 & 4) in each case the delay will be applied.

Physical Security

The Solo 3 is designed to provide protection against physical damage and complies with IK10 as defined in BS EN 62262.

If the charger detects the cover of the Solo 3 has been opened, enabling access to the internal hardware, an entry will be recorded in the Event Log section of the Pod Point App stating the date and time at which the cover was opened.

Data Security

The Solo 3 is protected to ensure that data contained upon it is secure and any identifiable information cannot be retrieved once it has been manufactured

- Only Pod Point signed firmware binaries can be installed on the device.
- Chargers validate the signature of the firmware on boot.
- All interfaces and access privileges not required for the charger to operate are disabled after manufacture and testing (STM Readout Protection Level = Level 2).
- Each Solo 3 has its own unique x.509 certificate injected during manufacture.
- The certificate is stored on encrypted flash, ensuring that it cannot be read from the charger.
- All application user interfaces are password protected.
- Passwords are user generated or where preset are unique to the charger and not based on any publicly identifiable information.
- Wi-Fi credentials entered on the Solo 3 can be removed via the option on the chargers Access Point page if needed, further information on this process is included in the Wi-Fi user guide for the charger.

Secure Communication

Remote functionality available with the Solo 3 can only be performed via the applications and services provided by Pod Point. Secure communication between the charger and Pod Points Charge Station Management System (CSMS) is ensured by:

- Communication via websockets encrypted using mTLS.
 - Chargers validate the issuing authority of the CSMS certificate and will only allow connectivity when the issuer is trusted.
 - Pod Point CSMS will only accept websocket connections from a device with a Pod Point issued certificate
 - Charger certificates are unique to the device.
- Rejection of any configuration updates sent to the charger that fail validation checks.

Security Updates

The firmware installed on the Solo 3 can be updated as new versions become available. The following process will apply when this occurs:

- Firmware updates are provided Over the Air (OTA) when the Solo 3 is connected to Wi-Fi.
- When a new version of firmware is available, this is indicated within the Pod Point Mobile App.
- When first installed a check is made for an available firmware update and if available the latest version will be installed.
- When future versions become available Pod Point will proactively update the firmware on the Solo 3 automatically.
- Firmware updates will be provided for 3 years starting from the point of installation.

The following mechanisms are used to check firmware validity and to ensure that only valid Pod Point firmware is installed and run on the Solo 3:

- The OTA process is only possible over the secure mTLS connection to the Pod Point CSMS. The Solo 3 verifies that the firmware binary is from a trusted source by validating the servers certificate.
- Firmware binaries are checked on device boot and when made available through an update to confirm that they have been correctly signed using a Pod Point firmware signing key.
- A failed validity check is registered in the security log of the Solo 3 which can be viewed within the Pod Point App.

Further Information

Should you have any concerns or problems relating to security please consult our vulnerability disclosure policy which can be found at:

<https://pod-point.com/legal/policies>

pod POINT