



## Eve Single S-line / Pro-line

Technical File

November 2022



## Table of contents

## Page

Table of contents	2
1 Description of Eve Single	3
2 Compliancy with Smart charging regulations	4
2.1 Smart charging	4
2.2 Electricity supplier interoperability	5
2.3 Loss of communications network access	5
2.4 Safety	6
2.5 Measuring system	7
2.6 Off-peak charging	8
2.7 Randomised delay	10
3 Compliance with Security requirements	11
4 References to other documents	18

# 1 Description of Eve Single

## Eve Single S-line

The Eve Single S-line is designed to offer genuine smart functionality for home charging. The compact casing contains a charging indicator LED and can be mounted to a wall or pole to offer a plug & play solution. It is available as a charging contact, or connected by a cable including cable storage. Internet connectivity is via ethernet, with online usage data available from our own management system or the one chosen by third parties.

## Eve Single Pro-line

Designed to be physically compact, without compromising any of Alfen’s smart functionality, the Eve Single Pro-line is suitable for business and home use and can be wall or pole mounted. The user interfaces with a colour screen with logo upload facility. An integrated RFID reader supports user identification and a MID-meter enables financial settlement. Internet connection is via LTE/ethernet, with data available via the chosen third party management system provider.

<b>Charge point make:</b>	Alfen ICU
<b>Charge point model:</b>	Eve Single S-line, Eve Single Pro-line
<b>Software version at point of sale:</b>	6.2 or higher
<b>Seller:</b> <i>Person responsible for compliance with the Regulations</i>	
<b>Manufacturer(s):</b> <i>If different to seller</i>	Alfen ICU B.V.
<b>Last update to technical file:</b>	November 2022
<b>Manual document version</b>	v4.2 – December 2021 (Installation and user manual) v3.0 – December 2021 (Quick installation guide)

Statement of compliance: included in the manual

A manual of Eve Single products is available:

- A) In the box
- B) Online: [www.alfen.com/downloads](http://www.alfen.com/downloads)

## 2 Compliancy with Smart charging regulations

### 2.1 Smart charging

This section explains how Alfen charge points meet the Smart charging requirements of the Regulation in the UK. The described functionalities are the same for all Alfen charge points.

Requirement	Technical solution adopted to meet the requirement
<p><b>Charge point is able to send and receive information via a communications network</b></p>	<p>Charge point uses OCPP protocol through both ethernet and mobile communications networks (sim slot available for the chargepoint operator). Connection with (home) energy management system available through ethernet network.</p>
<p><b>Charge point is able to respond to signals or other information received by it by:</b></p> <ul style="list-style-type: none"> <li>• Increasing or decreasing the rate of electricity flowing through the charge point</li> <li>• Changing the time at which electricity flows through the charge point</li> </ul>	<p>OCPP 1.6/J – full and certified implementation; includes smart charging module OCPP2.0.1/J – Same functionalities as supported by OCPP1.6</p> <p>Through smart charging profiles all controls are offered to the (re-)sellers of the products to include their services for DSR and/or Time of Use (ToU).</p> <p>Smart charging profiles capabilities allow for complex schedules:</p> <ul style="list-style-type: none"> <li>• Maximum stack level of charge profiles: 15</li> <li>• Max number of schedule periods per profile, defining time and charge rate: 100</li> <li>• Max number of charge profiles installed: 45</li> </ul>
<p><b>Charge point is capable of using this functionality to provide demand side response services, including response DSR services</b></p>	<p>Through OCPP smart charging profiles and (home) energy management system, the charge point can be part of a (response) DSR service. These services are not offered by the charge point, except for local smart charging solutions like Active Load Balancing.</p>
<p><b>Charge point has at least one user interface, incorporated in the charge point or otherwise made available to the owner</b></p>	<ul style="list-style-type: none"> <li>• Eve Single S-line: LED</li> <li>• Eve Single Pro-line: Display</li> <li>• All: MyEve App</li> </ul> <p>All: (Any) central management system</p>

## 2.2 Electricity supplier interoperability

Requirement	Technical solution adopted to meet the requirement
<p><b>Charge point is configured such that it will not cease to have smart functionality if the owner changes their electricity supplier</b></p>	<p>Alfen charge points differentiate from many others because they are “sim-lock free”, meaning that any operator can be connected.</p> <p>Charge point operation is outside scope of Alfen. This allows the owner of a charging station to switch freely between operator and providers.</p> <p>When standalone, the charge points remain fully operational with all local smart charging features available and the local charging schedule is still applied (Time of Use schedule)</p>

## 2.3 Loss of communications network access

Requirement	Technical solution adopted to meet the requirement
<p><b>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</b></p>	<p>Alfen charge points always try to reconnect automatically with the network.</p> <p>While offline, charging sessions will continue as if the product is online. The transaction will not be halted because the end-user was already authorized to charge. When the end-user stops the charge, either by swiping the same token (ID) or by removing the plug from their vehicle, all transaction data is stored locally until the charge point reconnects. When the product is online again, all transaction data is transmitted.</p> <p>It is also possible to sign in again by swiping a token (ID). Depending on the settings (to be defined by operator and/or owner), new charging transactions can be started in offline modus, for example when a previously used token was whitelisted. The charge point will verify if a token (ID) is available in its local database. It is also possible to accept all tokens in offline modus, to be configured by the owner. After reconnecting,</p>

the charge point will validate used tokens while offline and stops a session if a token was not authorized.

With regards to charging: When offline, the charge point remains fully operational with all smart charging features available.

Operators offering DSR services can send complete smart charging profiles with predefined schedules to the charge point. These can remain valid for a single transaction or have a recurrency (e.g. daily). As a result, charging is not affected at all. In addition, the charge point can dynamically adapt the rate of charge independent of any connection by using an interface with a local energy meter (modbus required). No remote connection with the DSR service is needed in such case.

In worst case scenario, where an operator or owner did not provide any fallback, a safe charging rate is applied until connection is re-established.

## 2.4 Safety

Requirement	Technical solution adopted to meet the requirement
<p><b>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.</b>  <b>“Relevant persons” means the owner, or an end-user of the relevant charge point who is not the owner.</b>  <b>“Specified operation” means:</b></p> <ul style="list-style-type: none"> <li>• <b>Overriding the default mode of charging during the default charging hours</b></li> <li>• <b>Overriding the provision of demand side response services</b></li> <li>• <b>Overriding the random delay</b></li> </ul>	<p>Charge points allow access to the local interface for the owner of the product. End-users cannot control the charge point, only use it. The operator can apply a service that must translate the end-user’s request to an appropriate smart charging profile.</p> <p>The owner can configure the charge point according to their wishes.</p> <p>In all circumstances, the charge point takes all measured and pre-set parameters into account as constraints to define the desired charge rate. These constraints cannot be overridden because they are safety related.</p>

Exception is the overriding functionality for the owner. This allows to override a smart charging profile offered by the DSR service (remote operator, or CPO). All other parameters and functionalities that are based on local measurements or settings, remain active. None of these local parameters can be overridden.

Overriding the random delay is allowed with immediate effect because the moment in time that an individual owner overrides the delay via the App is by itself random compared to other owners. While charging the charge point still adapts the rate of charge taking local constraints into consideration.

Overriding the random delay and DSR services are commands that are only valid for one charging session. This is to prevent the owner to accidentally forget to reactivate DSR services and run into high costs and avoid potential grid congestion. The owner has the possibility to define a local Time of Use schedule for the default charging hours of all upcoming transactions. This local schedule prevails over other (remotely received) schedules.

## 2.5 Measuring system

Requirement	Technical solution adopted to meet the requirement
<p><b>On each occasion it is used, the charge point measures or calculates:</b></p> <ul style="list-style-type: none"> <li>• <b>The electricity it has imported or exported (in watt-hours or kilowatt-hours)</b></li> <li>• <b>The amount of time for which it is importing or exporting electricity</b></li> </ul>	<p>Each chargepoint has its own energy meter to measure, save and/or send data in preferred format (energy (Wh) , current (A), Power (kW), voltage (V)) and a database to store transaction data, including time.</p> <p>Every charge point supports OCPP communication, all OCPP protocol versions offer this functionality.</p>
<p><b>The charge point is configured such that the owner can view the information in reference to:</b></p>	<p>Charge points share their data with central management systems. Users can benefit from</p>

<ul style="list-style-type: none"> <li>• Any occasion on which it was used to import or export electricity within the past 12 months</li> <li>• Any month within the past 12 months</li> <li>• The entirety of the last 12-month period</li> </ul>	<p>these services as long as the subscription is in place. These subscriptions are offered by charge point operators (CPOs) and/or the DSR services.</p> <p>In addition, the chargepoint saves all transactions locally and can provide them directly to the owner through the Alfen (MyEve) app.</p>
<p><b>The charge point is configured such that it can:</b></p> <ul style="list-style-type: none"> <li>• On each occasion it is used, measure or calculate every one second the electrical power it has imported or exported (in watts or kilowatts)</li> <li>• Provide this information via a communications network</li> </ul>	<p>Charge point reads available meter every 500ms and uses this information for internal calculations to allow safe charging transaction.</p> <p>Via the EMS (active load balancing) Modbus interface, data is refreshed every second.</p> <p>For remote central management systems, this is also possible but because this will clutter communication channels, it is strongly recommended to keep this information inside the charge point and use the DSR services' smart charging profiles instead. Local smart charging at the charger itself results in less communication and fastest response.</p>
<p><b>The charge point is configured such that:</b></p> <ul style="list-style-type: none"> <li>• The figures measured or calculated are accurate to within 10% of the actual figure</li> <li>• Any inaccuracies are not systematic</li> </ul>	<p>Time is synchronized via the heartbeat intervals as defined in OCPP</p> <p>Class B meters inside (<math>\pm 1\%</math>) and MID certified.</p>

## 2.6 Off-peak charging

Requirement	Technical solution adopted to meet the requirement
<p><b>The charge point:</b></p> <ul style="list-style-type: none"> <li>• Has pre-set default charging hours which are outside of peak hours</li> <li>• Offers the owner the opportunity to accept, remove, or change the default charging hours on first use</li> <li>• Offers the owner the ability to change, remove, or set default charging hours any time after first use</li> </ul>	<p>When a charge point is commissioned in the UK (using the MyEve configuration application), it assumes the following pre-set ToU schedule for default charging hours:</p> <p>Week days:</p> <p>ON: 12AM - 8AM  ON: 11AM - 4PM (meaning OFF: 8AM - 11AM)  ON: 10PM - 12PM (meaning OFF: 4PM - 10PM)</p> <p>Weekend: ON</p>



**unless the charge point is sold with a DSR agreement, configured to comply with the requirements of this agreement, and details of the agreement are included in the statement of compliance**

When 'ON', the charge point will maximise the charging rate based on configuration by the owner and information from e.g. local energy meters (active load balancing) or presence of other Alfen charge points.

When 'OFF', the end-user is allowed to start a charging transaction but there will be no transfer of energy until outside peak hours, or when the owner overrides the TuO charging schedule.

During commissioning, or at a later stage, the owner can change, remove or create a 'local charging profile' which overrides the DSR service (if applicable). The default charging hours are initialised through the commissioning on site using MyEve app and results in the ToU schedule as described above.

In all cases, the MyEve app is the trusted application to have the local charging profile updated, created or removed.

When 'ON', the charge point will always take into account measured or received constraints to ramp down (or up) the rate of charge to keep the installation and users safe.

As an alternative, a remote backend service may send a charging schedule with the purpose of being a ToU schedule immediately after commissioning but must take into account that the charge point only applies randomised delays to locally set ToU schedules. In case of remote schedules, the randomised delay must also be applied in that schedule by the central management system.

**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**

Via the MyEve App the owner can use “direct start” to override a Time of Use schedule (defining the default charging hours) or a randomised delay. This overriding action will be applied with immediate effect until the next on-peak default charging hour is reached. Then energy transfer will be stopped until the owner explicitly requests a ‘direct start’ again.

This overriding action will only work for the current transaction and when no energy transfer is taking place. When the transaction is finished, the DSR services or default charging hours are back in place for the next transaction.

## 2.7 Randomised delay

Requirement	Technical solution adopted to meet the requirement
<p><b>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</b></p>	<p>The backend service should provide DSR services and or ToU schedules. Before sending these schedules, a random delay can be applied to the schedule in preparation for the next transaction.</p> <p>Each charge point applies a default randomised delay of up to 600 seconds when a local Time of Use schedule is active. This delay is applied every instance where charging is started or when the charge rate is changed as part of the default charging hours.</p> <p>This parameter is available as:</p> <ul style="list-style-type: none"> <li>• OCPP configuration for each charge point</li> <li>• Configuration in MyEve app</li> </ul> <p>It can be configured in seconds.</p>
<p><b>The charge point is configured such that the maximum duration of this delay can be remotely increased to up to 1800 seconds if required</b></p>	<p>Offered through the backend services and MyEve app</p> <ul style="list-style-type: none"> <li>• Possible values for the randomised delay: 0-3600 (seconds)</li> <li>• Default value: 600 (seconds)</li> </ul>

	<p>The randomised delay is not applicable to charging profiles offered through backend services. The backend service should provide DSR services and or ToU schedules with a randomised delay.</p>
<p><b>The charge point is configured such that the random delay will not operate where:</b></p> <ul style="list-style-type: none"> <li>• <b>The owner or another relevant end-user has manually overridden it</b></li> <li>• <b>An equivalent random delay has already been applied to the operation of the relevant charge point</b></li> <li>• <b>The charge point is responding to a response DSR service</b></li> </ul>	<p>The randomised delay is only applied for relevant setpoints of the default charging hours.</p> <p>This means that the randomised delay is not applied if the change of charging rate is a result from:</p> <ol style="list-style-type: none"> <li>a) A local measurement (safety)</li> <li>b) Command from e.g. an EMS (safety)</li> <li>c) A smart charging schedule (OCPP), meaning a demand side response (DSR) or response DSR service is active</li> <li>d) Direct start via MyEve App</li> <li>e) Any other event that may cause safety risks</li> </ol> <p>Referring to c): even with the OCPP smart charging profile in place, the owner or operator has to remove the local ToU schedule to explicitly inform the charge point that the DSR service is leading.</p>

### 3 Compliance with Security requirements

Requirement	Technical solution adopted to meet the requirement
<p><b>General principles</b></p> <p><b>The charge point is designed, manufactured, and configured to provide appropriate protection:</b></p> <ul style="list-style-type: none"> <li>• <b>Against the risk of harm to, or disruption of the electricity system</b></li> <li>• <b>Against the risk of harm to, or disruption of, the charge point</b></li> <li>• <b>For the personal data of the owner and any other end-user of the relevant charge point</b></li> </ul>	<p>Data stored on the charging station can only be obtained via a local interface, using the MyEve App.</p> <p>This is a protected interface to prevent other applications to access the data.</p> <p>As an alternative, data is sent to a remote management system, selected by the owner. It is possible to protect this communication channel using an encryption layer (TLS1.2). The charge point does not store direct personal data of the owner. The transaction data is protected by password access and used via the MyEve app.</p>

	<p>Data stored on the charge point is encrypted and cannot be accessed without the mentioned tool.</p>
<p><b>Passwords</b>  <b>The charge point is configured such that where passwords are used on it:</b></p> <ul style="list-style-type: none"> <li>• <b>The password is unique to the charge point and not derived from, or based on, publicly available information, or is set by the owner</b></li> <li>• <b>The password cannot be reset to a default password applying to both the charge point and other charge points</b></li> </ul>	<p>Each charge point is delivered with a unique random code pair, being:</p> <p><b>Default Password</b>      Random, unrelated to any product parameter.  Length: 12 alphanumeric characters/ special characters</p> <p>Characters excluded for readability purposes:  - "l" (lowercase L)  - "I" (capital i)  - "O" (capital o)  These are replaced by special character @, #, \$, &amp; to keep sufficient complexity</p> <p><b>Password Recovery Code</b>      Random, unrelated to any product parameter.  Length: 16 alphanumeric characters</p> <p>These codes are intended for the owner of the charge point and need to be kept in a safe location.</p> <p>It is strongly recommended to replace and (regularly) update the Default Password with a owner-defined password. When forgotten, the owner can apply the Password Recovery Code to reinstate the Default Password.  As this code pair is unique for each charge point, there is no possibility to use either one of them to access other charge points.</p> <p>Note: owners can decide to use the same user-defined password for several charge points. This is however not recommended. It is to the owners' discretion to decide otherwise.</p>
<p><b>Software</b>  <b>The charge point incorporates software which is able to be securely updated using adequate cryptographic measures to protect against cyber attack</b></p>	<p>Firmware is encrypted and signed by Alfen.  Encryption: RSA key with 2048 bit length</p> <p>All other firmware is rejected by the charge point</p>

**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**

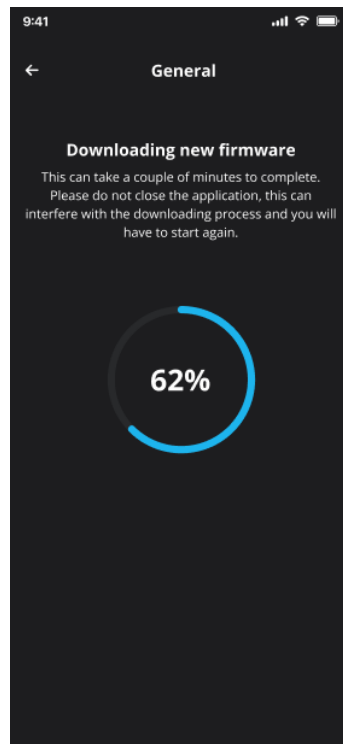
Each charge point is delivered with the latest firmware. When being commissioned, the MyEve will have the latest firmware available for each station via the Alfen backend.

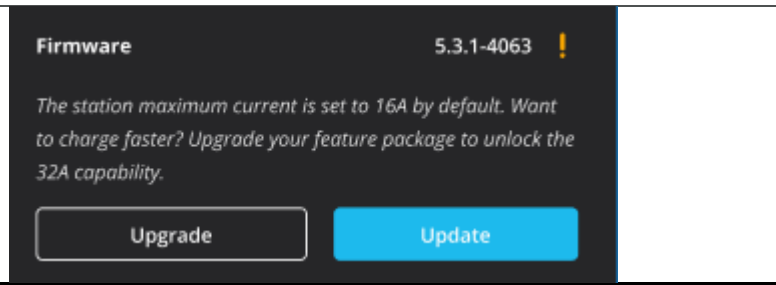
Only when the firmware originates from Alfen, it will be applied by the charge point. Otherwise it is discarded.

The MyEve app provides notifications about available firmware updates for the charge point. The user of the MyEve app can request to update the firmware with a single click.

Alternative: the DSR service provider, or Chargepoint Operator (CPO) can have the latest firmware installed as part of their services. Alfen offers the firmware package to all known backend partners for distribution across their networks. As such, the backend partners receive the firmware with the owns certificates pre-installed.

MyEve app screenshots:



																					
<p><b>Software</b> The charge point is configured such that:</p> <ul style="list-style-type: none"> <li>• It verifies via secure boot mechanisms that its software has not been altered other than in accordance with a validated software update</li> <li>• 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</li> </ul>	<p>The charge point has an immutable bootloader that:</p> <ul style="list-style-type: none"> <li>• Checks if a firmware update or rollback is requested.</li> <li>• Ensures write protection of memory containing the application</li> <li>• Checks the metadata of the application firmware.</li> <li>• Starts the application program when metadata is correct</li> </ul> <p>If metadata cannot be verified, the previous firmware is put back into place.</p>																				
<p><b>Sensitive security parameters</b> The charge point is configured such that:</p> <ul style="list-style-type: none"> <li>• Security credentials stored on the charge point are protected using robust security measures</li> <li>• Software does not use hard-coded security credentials</li> </ul>	<p>Credentials are stored hashed and salted in a database located in the CPU flash memory, which in turn is protected with RDP #2 against external manipulation.</p> <p>Instead of hardcoded credentials, the software uses a random password, unique per charger to allow access to the device.</p>																				
<p><b>Secure communication</b> The charge point is configured such that communications it sends are encrypted</p>	<p>The charge point supports the following secure communications for OCPP1.6</p> <table border="1" data-bbox="655 1585 1434 2000"> <thead> <tr> <th>Description</th> <th>Value</th> <th>Charging station authentication</th> <th>Central System Authentication</th> <th>Communication Security</th> </tr> </thead> <tbody> <tr> <td>Default</td> <td>0</td> <td>*</td> <td>*</td> <td>*</td> </tr> <tr> <td>Unsecure Transport with Basic Authentication</td> <td>1</td> <td>HTTP Basic Authentication</td> <td>-</td> <td>-</td> </tr> <tr> <td>TLS with Basic Authentication</td> <td>2</td> <td>HTTP Basic Authentication</td> <td>TLS authentication using certificate</td> <td>Transport Layer Security (TLS)</td> </tr> </tbody> </table>	Description	Value	Charging station authentication	Central System Authentication	Communication Security	Default	0	*	*	*	Unsecure Transport with Basic Authentication	1	HTTP Basic Authentication	-	-	TLS with Basic Authentication	2	HTTP Basic Authentication	TLS authentication using certificate	Transport Layer Security (TLS)
Description	Value	Charging station authentication	Central System Authentication	Communication Security																	
Default	0	*	*	*																	
Unsecure Transport with Basic Authentication	1	HTTP Basic Authentication	-	-																	
TLS with Basic Authentication	2	HTTP Basic Authentication	TLS authentication using certificate	Transport Layer Security (TLS)																	

	<table border="1"> <tr> <td data-bbox="660 344 855 474"> <b>TLS with Client Side Certificates</b> </td> <td data-bbox="855 344 935 474">3</td> <td data-bbox="935 344 1078 474">           TLS authentication using certificate         </td> <td data-bbox="1078 344 1222 474">           TLS authentication using certificate         </td> <td data-bbox="1222 344 1428 474">           Transport Layer Security (TLS)         </td> </tr> </table>	<b>TLS with Client Side Certificates</b>	3	TLS authentication using certificate	TLS authentication using certificate	Transport Layer Security (TLS)
<b>TLS with Client Side Certificates</b>	3	TLS authentication using certificate	TLS authentication using certificate	Transport Layer Security (TLS)		
<p><b>Data inputs</b> The charge point is configured such that:</p> <ul style="list-style-type: none"> <li>• Data inputs are verified so that the type and format of the data is consistent with that expected for the function</li> <li>• If such data cannot be verified, it is discarded or ignored by the charge point in a relevant manner</li> </ul>	<p>More information is available in document “secure back office communication” dd. 2019-08-26</p> <p>Upcoming OCPP2.0.1 implementation has a security implementation similar to OCPP1.6 SE. These messages allow to make full use of the charge point’s secure features in relation to OCPP communication (with DSR or CPO).</p> <p>The charge point verifies data fields for correctness and if incorrect, or of unsupported format or size, the message is discarded.</p>					
<p><b>Ease of use</b> The charge point is configured to minimise the inputs required from the owner in connection with its set-up and operation</p>	<p>MyEve App must be used to commission and configure the charge point.</p> <p>To provide easy setup, the MyEve uses a ‘wizard’-like approach to commission new charge points to guide the user through all relevant settings without skipping important settings. After the wizard, the charge point is ready to use.</p>					
<p><b>Ease of use</b> The charge point is configured such that any personal data can be deleted from it by the owner without undue difficulty</p>	<p>Using the MyEve App, the owner can delete whitelist database and transaction database directly from the chargepoint.</p>					
<p><b>Protection against attack</b> The charge point is designed and manufactured to provide an adequate level of protection against physical damage to the charge point</p>	<p>IK10 rated enclosure</p>					
<p><b>Protection against attack</b> The charge point incorporates a tamper-protection boundary to</p>	<p>Tamper detection will be placed on the enclosure.</p>					

<p><b>protect the internal components of the charge point</b></p>	<p>When the chargepoint is powered on and opened, it assumes an attempt to breach the digital interfaces and reports a security notification</p> <ul style="list-style-type: none"> <li>a) To OCPP central management system, if present</li> <li>b) On the display, if present</li> <li>c) In the Alfen (MyEVe) app</li> </ul> <p>The notification can be cleared by the owner.</p>
<p><b>Protection against attack</b> 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</p>	<p>All user interfaces that are not in use, are disabled.</p>
<p><b>Protection against attack</b> The charge point is configured such that:</p> <ul style="list-style-type: none"> <li>• If there is an attempt to breach the tamper-protection boundary, the owner is notified</li> <li>• Its software runs with only the minimum level of access privileges required to deliver functionality</li> <li>• 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</li> <li>• Software services are not available to the owner unless necessary for the relevant charge point to operate</li> <li>• 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</li> </ul>	<p>The charge point will report an attempt to breach tamper detection to the backoffice, writes this event in the security log and notifies the owner through its display (if present)</p> <p>Reset by owner after logging in using their password and release the tamper detection event.</p> <p>All user interfaces and functionalities that are not in use, are disabled by default (firmware always runs with minimum level of access to be functional/ operational).</p>
<p><b>Security log</b></p>	<p>The charge point has a security log that registers:</p> <ul style="list-style-type: none"> <li>• Ethernet cable disconnections/connections</li> </ul>



**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).**

- Attempts to login with incorrect password
- Attempts to send invalid or replayed messages on the OCPP back office interface
- Attempts to change configuration without proper authorization

## 4 References to other documents

Certificate	Date of test	Outcome	Certificate number	Notes
<b>OCP 1.6 Full Certificate</b>	December 19, 2019	Passed	OCA.0016.0003.CS	Tested by DEKRA on behalf of Open Charge Alliance (OCA). Certificate available upon request
<b>IEC61851-1 certificate</b>	July 20, 2018	Passed	NL-53552	Tested by DEKRA

Document title	Version	Related to	Notes
<b>Security Design document</b>	2.5	Schedule 1, cyber security	Confidential document, only available with NDA in place and consent from Chief Information Security Officer
<b>Secure back office communication</b>	08-26-2019	Schedule 1, cyber security	
<b>ENCS- EV Charging Systems Security Requirements</b>	June 2021	Schedule 1, cyber security	<a href="#">News item Vattenfall, together with Alfen Twin (shared platform with Eve Double and firmware with Eve Single S-line, Eve Single Pro-line and Eve Double Pro-line)</a>