EV-301-2022

Security requirements for procuring EV charging stations

Version 2022v0.3

17 February 2022

This document was produced in the ENCS program on Security Architectures. This program support ENCS members in selecting and implementing technical security measures for systems and their components. The document is part of a series of requirements available through the ENCS portal (https://encs.eu/documents):

This document is shared under the Traffic Light Protocol classification:

TLP White – public

The European Network for Cyber Security (ENCS) is a non-profit membership organization that brings together critical infrastructure stake owners and security experts to deploy secure European critical energy grids and infrastructure.

Version History

Date	Version	Description
April 2016	1.0 (2016v1.0)	Initial release of requirements from Elaad Cyber-security project
December 2019	2.0 (2019v1.0)	Final version in ENCS member project on procuring secure equipment
7 December 2021	2021v0.1	First draft of updated requirements
1 February 2022	2022v0.2	Second draft with integrated security context
17 February 2022	2022v0.3	Draft updated based on ENCS member feedback

Table of Contents

1 Introduction

This document gives security requirements that Charge Point Operators (CPO) can use when procuring new charging stations.

CPOs are controlling increasingly more electrical load. To support the rapid growth in electric vehicles (EVs), hundreds of thousands of charging stations are being placed throughout Europe, most of them being remotely controlled by CPOs. In this way, larger CPOs are already controlling hundreds of megawatts of demand, comparable to a large gas power plant. And the controlled load will only grow in the future.

The cyber-attacks on Ukrainian grid operators [1] have shown that there are hackers that have the skills and motivation to disrupt the power grid. But this also means that CPOs are a target for cyber-attacks. If attackers gain control of a CPO’s infrastructure, they could switch the power on the connected charging stations. Such an attack would not only hurt the CPOs themselves. The switching could also cause grid imbalances in the supply and demand for electricity and, possibly, power outages. If smart charging is used, attackers may force charging stations to use more power than assigned to them, which could force grid operators to switch of power in some areas and in the worst case could damage transformers and power lines.

To mitigate these risks, ENCS and ElaadNL created in 2019 a set of requirements that CPOs could use in their procurement documents for charging stations. In 2022, ENCS has created an updated version to harmonize ENCS requirements, include the security context and to include a mapping to IEC 62443.

This document provides a harmonized set of security requirements that charge point operators use directly in their procurement documents for charging stations. They are designed to fit into the processes and procedures already in place in the organizations and to find a good balance between security and the operational impact.

This requirement set should reduce time and effort in developing requirements, as they are already freely available. It ensures the requirements are feasible, as they have been tested in a market survey and in previous tenders by other operators. It also reduces implementation costs, because vendors get a common baseline from the clients to aim at and only need to implement the security requirements once.

1.1 Intended use of the document

This document gives requirements for procuring electrical vehicle charging stations that are controlled remotely by a Charge Point Operator. This includes charging stations in public places, semi-public charging stations in parking garages, and even some privately owned charging stations.

The EV charging stations are connected to a charging station management system (CSMS). The charging station sends information on transactions to the CSMS for billing.

The charging stations may be used for smart charging. In that case, the CSMS adjusts the charging speed to help grid operators solve load balancing or congestion problems in the electricity grid.

The payment terminal is considered as an external device, out of scope for the security requirements. Secure payment is of course critical for charging stations. But different payment solutions are used by different charge point operators and several new solutions are now under development. So, including requirements on payment security would make this document quickly outdated.

This document is aimed at standalone charging stations that communicate directly with the CSMS. In parking plazas, some charging stations may instead be connected to the CSMS through a local controller. The requirements may then be used for the local controller. But the threats to the communication between the local controller or between the different charging stations in the charging plaza are not considered here.

Threats to communication between a charging station and a local energy management system (EMS) are also not considered. No requirements are included to protect this communication.

1.2 Intended operational environment

Figure 1 shows the reference architecture for the EV charging station used in this document.

The charging stations are connected to the CSMS over a wide-area network (WAN). Usually, the WAN is a wireless mobile network, such as a GPRS, CDMA, or LTE network. The communication on the WAN network may be protected through network segregation, for instance through a private APN. Such segregation would be recommended, certainly for larger charge point operators. But in this document, no assumptions are made on the security measures on the WAN. The network is considered untrusted.

Charging stations can deployed on various locations. They may be deployed in the street or in public parking spaces. They can also be deployed in semi-public parking garages or in private parking spaces. Charging stations may be deployed individually or as part of a charging plaza. Generally, the charge point operators cannot control or monitor access to the locations. So, the charging stations are exposed to physical attackers.

The charging station is maintained by engineers. They can maintain the charging station locally through the local maintenance interface or remotely through the CSMS. Engineers only visit the charging stations when there are problems or there is scheduled maintenance.

1.3 Security features

The security requirements are designed to offer the following security features to electrical vehicle charging stations:

- Securing access to the device from the CSMS over the WAN network by enforcing authentication and cryptographically protecting the communication.
- Protecting access to the configuration and firmware on the device by engineers through access control, logging configuration changes, and checking firmware signatures before installation.
- Protecting the device from exploits against software vulnerabilities through hardening, allowing remote updates, and requiring secure development processes at the supplier.

This document gives requirements for procuring remotely controlled charging stations. The architecture concerns the interfaces to the charging station and the users on these interfaces (see Figure 1). The architecture does not consider the internal working of the charging station. The measures are aligned with ISO 27001:2013 [2] and cover the following sections from Annex A of that document:

- Access control (A.9)
- Cryptography (A.10)
- Physical and environmental security (A.11)
- Operations security (A.12)
- Communication security (A.13)
- System acquisition, development, and maintenance (A.14)
- Supplier relationships (A15)

Each subsection gives requirements used to meet an objective in ISO 27001 Annex A. The objective number is given in square brackets.

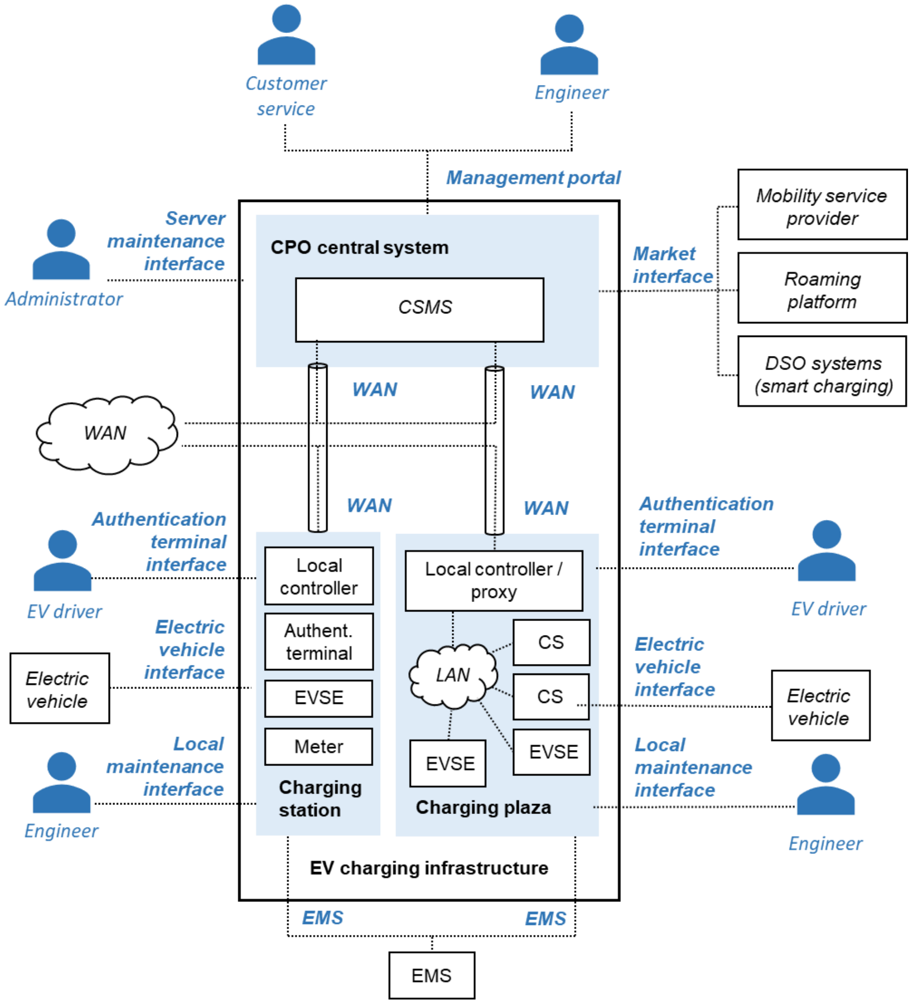

Figure 1: Reference architecture for the EV charging station, showing its users and interfaces.

Using the requirements

The security requirements are part of a larger approach to creating secure systems, both when building new systems or updating existing systems. It consists of the following steps:

1. Perform a **security risk assessment** to understand the threats to the system and the impact these risks can have on it. An assessment of the typical risks is available for EV charging infrastructure in [3].
2. Design a **security architecture** that selects technical security measures to mitigate the risks. Measures should be chosen for the entire system, as this is usually more effective than choosing measures per component. The architecture can act as a blueprint for system integrators and the departments maintaining the system. A recommended security architecture is available for EV charging infrastructure in [4].
3. Derive **requirements for components** from the security architecture that can be used to develop or procure the components. This document gives security requirements for EV charging stations. The requirements are mapped to the IEC 62443-4-2 standard [5], used by some vendors, in Appendix A.
4. **Test the components** to check that they meet the security requirements. In a procurement process, such tests should be part of the selection phase. A test plan for EV charging stations is available in [6].
5. **Test the system** to check that it is deployed according to the architecture and mitigates the risks. The implementation of the architecture can be checked using a technical audit. Mitigation of the risks can be checked using penetration and red team tests simulating the threats.

These steps ensure that a secure system is delivered. But after that, it still needs to be operated securely. Processes and procedures should be set up to securely maintain the system, manage keys and passwords, and respond to incidents.

To ensure the quality of the processes and procedures, it is recommended to use an information security management system, for instance, based on the ISO/IEC 27001 [2]. To support this, the architecture is organized by the security objectives in ISO/IEC 27001 Annex A.

2 Security context

This section describes the security context of the charging stations in terms of the assets processed by them, the access control applied to these assets, and the threats that may compromise the assets. The security objectives in Section 3 are designed to counter these threats.

2.1 Assets

The main purpose of a charging station is to charge electric vehicles and send usage information per customer to the CSMS for billing. Therefore, the primary information assets for the charging station are the information sent to or received from the CSMS:

- Transaction data from EV drivers, such as the ID of the EV driver
- Meter values
- Tariffs

Additionally, the charging station may be used for smart charging, in which the charging speed is adjusted to help with load balancing or congestion management in the electricity grid. If smart charging is used, the CSMS may send charging profiles to the charging station to set the maximum charging speed.

The charging station is configured remotely through the CSMS or locally by the charge point operator's engineers. The information assets needed for this are the firmware, and the stored configuration, including the communication settings. Additionally, engineers may need the operational logs of the device to analyze and fix problems with the device.

For security, key information assets are the security logs and the keys and passwords stored on the charging station. These include the passwords used by engineers to log in and the keys used for authentication and communication security on the WAN.

Credit and debit card information or other information for transaction authorization (such as RFID data or PIN codes) is not considered an asset for the charging station. Such information is processed by the payment terminal, which is considered out of scope (Section 1.1). The data should be encrypted and authenticated when it is sent through the charging station (see objective SO-CM3 in Section 3.2.2).

2.2 Access control policy

Table 1 lists the users that are authorized to access the charging station and the access they require. See Figure 1 for the interfaces. Users can be both human users and other systems accessing the charging station. The access control policy should be designed to implement the principle of least privileges, so that each user group can only access the functions it requires.

Table 1 User groups on the device.

User	Required access	Interface
Charging Station Management System (CSMS)	• Collect transaction data and meter values for billing • Set tariffs • Configure the charging station • Restore the charging station from a backed up configuration • Update the firmware • Monitor operational logs • *Optional:* Send charging profiles	WAN
Engineer	• Configure the charging station • Restore the charging station from a backed up configuration • Update the firmware • Analyze the operational logs	Local maintenance
EV driver	• Authenticate for charging • *Optional:* Pay for charging	Authentication terminal
Electric vehicle	• Control the charging • *Optional:* authenticate for charging	Electric vehicle

2.3 Threats

The charging station should be protected against the following threats. These threats have been identified in the security risk assessment for EV charging infrastructure [3].

Unauthorized access on WAN, local maintenance, electric vehicle interface, or authentication terminal interfaces

An attacker gains access to WAN, local maintenance, electric vehicle, or authentication terminal interfaces and then gains unauthorized access to the charging station. With this access they may stop charging, tamper with transactions and meter values, set incorrect tariffs or charging profiles or change the configuration or firmware.

Unauthorized charging

An attacker charges an electric vehicle without authorizing on the payment terminal.

Unauthorized physical access

An attacker gains physical access to the charging station and uses the physical access to gain logical access. Attackers may log in on one of the ports or physically tamper with the hardware. With this access they may stop charging, tamper with transactions and meter values, set incorrect tariffs or charging profiles or change the configuration or firmware. They may also try to gather financial information, such as credit card and debit card numbers or PIN codes, sent between the payment terminal and payment company through the charging station.

Data modification on WAN

An attacker gains access to the WAN network and then modifies information sent to or from the charging station. In this way, they may stop charging, tamper with transactions and meter values, set incorrect tariffs or charging profiles or change the configuration or firmware.

Data disclosure on WAN

An attacker gains access to the WAN network and then eavesdrops on information sent to or from the charging station. In this way, they may gain confidential information sent between the charging station and CSMS, such as meter values or the configuration of the charge point operator's system.

Network denial-of-service attack on the WAN interface

An attacker gains access to the WAN interface and disrupts the normal operation of the charging station, for instance by sending malformed messages or flooding the device with data. In this way, they may stop charging, prevent transaction data, meter readings, and logs being sent to the CSMS, and charging profiles, configurations, and firmware updates being sent to the charging station.

Exploit of software vulnerability

An attacker bypasses the access control measures on an interface by exploiting a software vulnerability. With the access gained they may stop charging, tamper with transactions and meter values, set incorrect tariffs or charging profiles or change the configuration or firmware.

Firmware modification

An attacker modifies the firmware before it is installed on the charging station. The firmware could be modified at the developer or in transit between the developer and the device. In this way, attackers may, for instance, install backdoors or logic bombs in the charging station that would allow them to stop charging, tamper with transactions and meter values, or set incorrect tariffs or charging profiles.

Harmful actions by engineers

Engineers with authorized access, incidentally or on purpose, perform actions that are harmful to the charging station or the EV charging infrastructure. They may, for instance, make incorrect changes to the configuration or install the wrong firmware.

Loss of stored data

The data stored on the charging station is deleted or becomes corrupted through mistakes by engineers or intentional actions from an attacker that has gained access.

3 Security objectives

This section provides security objectives that should be met to implement the access control policy in Section 2.2 and counter the threats described in Section 2.3.

The objectives are split into objectives to the charging station (Section 3.1) and objectives to the operational environment (Section 3.2). The objectives to the device can be met by the device if it implements the baseline security requirements in Section 4. The objectives to the operational environment are additional organizational and technical measures that the charge point operator should take to securely operate the devices.

3.1 Objectives for the charging station

To implement the access control policy in Section 2.2 and counter the threats described in Section 2.3, the charging station should meet the following security objectives. These objectives are covered by the baseline security requirements, as demonstrated in Section 3.4.

AC4 Role separation for EV drivers, engineers, CSMS, and electric vehicles

The charging station can enforce access control with separate roles for EV drivers, engineers, the CSMS, and electric vehicles, so that each user can only access the functions they need for their role. The EV drivers, engineers, the CSMS, and electric vehicles identify to the charging station with information that allows the charging station to determine their role. The charging station authenticates the user's role and assigns them access rights based on the role. The charging station uniquely identifies itself to the users and allows them to authenticate it.

PH2 Protection against moderate physical attacks

The device can prevent attackers with low resources or low motivation and with physical access to the device from gaining access on external or internal interfaces. The device generates an alarm to the central systems when such attackers try to access its insides.

CM1 Cryptographic protection of communication confidentiality and integrity on WAN

The charging station shall cryptographically protect the integrity and confidentiality of communication on the WAN interface. The measures shall allow to verify the source of messages and protect against replay and man-in-the-middle attacks.

CM2 Resilience of ongoing charging transactions against denial-of-service attacks on the WAN interface

The device shields ongoing charging transactions from denial-of-service attacks on the WAN interface, so that these functions keep working if the device is flooded with data or malformed messages are sent.

MA3 Automated management

The device can be managed automatically by the central systems. The central systems can remotely and automatically:

- update passwords and keys
- update the software or firmware
- restore the device from a backed-up configuration

The device allows the confidentiality and integrity of the passwords, keys, software, firmware, and configurations to be protected cryptographically during transport. The device checks the authenticity of firmware or software through digital signatures. The device automatically triggers updates of keys or credentials during commissioning or when they are about to expire.

The device shall be delivered by the supplier in a secure configuration. Unneeded functions are disabled, and security features of the underlying hardware and operating system are used whenever possible.

MO2 Collecting security events from the central system

The device logs security events, such as access control events, and changes to the configuration and firmware. The device can store the logs locally and allows the central systems to collect them. Logs are protected against tampering. The device supports time synchronization to have reliable timestamps for events.

SC2 Protection of assets at developer against advanced threats

The developer protects the confidentiality, integrity, and availability of any assets that could compromise the security of the device against simple threat actors. The vendor shall have a certified ISMS covering these assets.

SC3 Secure development

The developer of the device minimizes the likelihood of software vulnerabilities by implementing secure development processes, including secure programming practices, security testing during development, and vulnerability handling.

3.2 Objectives to the operational environment

Besides the objectives the charging station should meet, the operational environment should meet the following objective to ensure the organizational security policies can be followed and threats are mitigated.

3.2.1 Organizational security objectives

The following organizational security objectives are especially important to operate the charging station securely. It would be recommended to implement these controls through an information security management system (ISMS), such as ISO/IEC 27001.

OR1 Personnel security

The charge point operator should ensure that the engineers with authorized access to the charging stations are competent and trustworthy, for instance through:

- Screening
- Training and awareness
- Disciplinary processes
- Monitoring by management

Related controls from ISO/IEC 27001: 7.1.1 Screening, 7.1.2 Terms and conditions of employment, 7.2.1 Management responsibilities, 7.2.2 Information security awareness, education, and training, 7.2.3 Disciplinary process, 7.3.1 Termination or change of employment responsibilities

OR2 Security monitoring and incident response

The charge point operator monitors security events on the device and can respond to them. They gather security logs from the devices centrally, for instance, in a SIEM. They establish procedures, use cases, and rules to find incidents in the logs. And they establish a process for responding to the incidents and minimizing the impact.

Related controls from ISO/IEC 27002: 12.4.1 Event logging, 12.4.3 Administrator and operator logs, 16.1.4 Assessment of and decision on information security events, 16.1.5 Response to information security incidents

OR3 Key and password management

The charge point operator manages the keys and passwords of the charging stations, so that they are properly protected and can be updated when needed.

Related controls from ISO/IEC 27002: 10.1.2 Key management

OR4 Vulnerability management

The charge point operator can monitor vulnerabilities in the charging station software and firmware, assess the risks of the vulnerabilities, and mitigate the high-risk vulnerabilities.

Related controls from ISO/IEC 27001: 12.6.1 Management of technical vulnerabilities.

Remark: Vulnerabilities will be found in the firmware during the lifetime of the charging station. Many charging stations rely on open-source libraries and applications for which vulnerabilities are regularly found and published in public databases. Often exploits are readily available.

Charge point operators will hence need to set up processes first, to monitor vulnerabilities in the software used. Vulnerabilities should be reported by the supplier as part of vulnerability handling process (objective SC3 in Section 3.1). The operator then needs to assess the risks of vulnerabilities to their system. In case of a high-risk vulnerability, they need to be able to roll out security updates quickly.

OR5 Backup process for charging station configurations

The charge point operator has a process to back up the configurations of the charging stations at their central systems. Older versions of the configurations are kept, so that it is possible to revert to them in case of issues.

Related controls from ISO/IEC 27001: 12.3.1 Information backup

3.2.2 Technical security objectives at system level

The following technical security objectives should at least be met at system level to operate the charging stations securely. For a full set of recommended security measures at system level, see the *Security architecture for electric vehicle charging infrastructure* [4].

SO-AC7 Authorization on the payment terminal

EV drivers shall identify themselves to the payment terminal, in such a way that the payment companies can bill the electricity consumed. The payment terminal shall authenticate the user before authorizing the charging station to start the charging transaction.

SO-PI1 Physical impact limiting

Communication between charging stations and from charging stations to the central system is restricted to what is needed, so that the impact of a compromise of one charging station can be limited to that charging station.

Remark: Communication between charging stations can be blocked on the telecom network by blocking SIM-to-SIM communication.

Additionally, if symmetric keys or passwords are used, it is recommended to use unique credentials for authentication to the charging stations over the WAN. In this way, if an attacker compromises one charging station, they do not gain credentials that they can use to log in on other charging stations.

SO-CM3 End-to-end security for transaction authorization information between the payment terminal and the payment company

The confidentiality and authenticity of information used to authorize transaction, such a credit or debit card information or PIN codes, is end-to-end protected by cryptographic measures between the payment terminal and the systems of the payment company.

3.3 Rationale for the security objectives

Table 2 shows which security objectives are meant to protect against which threats. A further explanation for each threat is given below.

Table 2: Mapping of threats to security objectives.

	Unauthorized access on WAN, local maintenance, or electric vehicle interfaces	Unauthorized charging	Unauthorized physical access	Data modification on WAN	Data disclosure on WAN	Network denial-of-service attack	Exploit of software vulnerability	Firmware modification	Harmful actions by engineers	Loss of stored data
AC4 Role separation for EV drivers, engineers, the CSMS, and electric vehicles	■									
PH2 Protection against moderate		■	■							

	Unauthorized access on WAN, local maintenance, or electric vehicle interfaces	Unauthorized charging	Unauthorized physical access	Data modification on WAN	Data disclosure on WAN	Network denial-of-service attack	Exploit of software vulnerability	Firmware modification	Harmful actions by engineers	Loss of stored data
physical attacks (SL-2)		🟦	🟦							
CM1 Cryptographic protection of communication confidentiality and integrity on WAN				🟦	🟦					
CM2 Resilience of charging transaction against denial-of-service attacks on the WAN interface						🟦				
MA3 Automated management	🟦						🟦	🟦		🟦
MO2 Collecting security events from the central system	🟦		🟦					🟦	🟦	
SC2 Protection of assets at developer against advanced threats								🟦		

	Unauthorized access on WAN, local maintenance, or electric vehicle interfaces	Unauthorized charging	Unauthorized physical access	Data modification on WAN	Data disclosure on WAN	Network denial-of-service attack	Exploit of software vulnerability	Firmware modification	Harmful actions by engineers	Loss of stored data
SC3 Secure development							🟦			
OR1 Personnel security									🟦	
OR2 Security monitoring and incident response	🟦		🟦					🟦		
OR3 Key management	🟦									
OR4 Vulnerability management							🟦			
OR5 Backup process for charging station configurations										🟦
SO-AC7 Authorization on the payment terminal		🟦								

	Unauthorized access on WAN, local maintenance, or electric vehicle interfaces	Unauthorized charging	Unauthorized physical access	Data modification on WAN	Data disclosure on WAN	Network denial-of-service attack	Exploit of software vulnerability	Firmware modification	Harmful actions by engineers	Loss of stored data
SO-PI1 Physical impact limiting	🟦		🟦							
SO-CM3 End-to-end security for transaction authorization information between the payment terminal and the payment company			🟦							

3.3.1 Protecting against unauthorized access on the LAN, WAN, local maintenance, or electric vehicle interface

The primary measure against unauthorized access on the WAN, are the access control measures for the SCADA and central maintenance system (**AC4**). These should ensure that only these authorized systems can access the device. Automated management of keys and passwords (**MA3**, **OR3**) ensures that the credentials can be regularly updated, reducing the risk of a compromise. Failed and successful attempts are logged (**MO2**) so that local access attempts can be detected and responded to (**OR2**).

Attacker may try to bypass the access control in three ways. First, they could try to access other network services on the WAN, not protected by the access control measures. Hardening (**MA3**) ensures these network services are closed.

Second, attackers could try to access the device from a compromised charging station at another field location. The charging station may for instance be compromised by a physical attack. The compromised charging stations would have access to the WAN network and may give attackers access to the credentials of the CSMS. So, it is important that charge point operators block direct communication between charging stations at different locations to limit the impact of such attacks (**SO-PI1**).

Third, attackers could try to exploit a software vulnerability in the device. This threat is mitigated by the objectives in Section 3.3.6.

3.3.2 Protecting against unauthorized charging

The charging stations is protected against unauthorized charging primarily through authentication on the payment terminal (**SO-AC7**). The authentication mechanism is out of scope for the security requirements in this document.

Attacker may bypass the authentication by physically breaking open the charging station. Physical protection measures (**PH2**) should protect against moderate attacks, so that this type of attack becomes less interesting. The possible money saved from free charging would not weigh up against the time needed to break into the charging station.

3.3.3 Protecting against unauthorized physical access

As the charging station may be placed in a public or unprotected location, it should be protected against moderate physical attacks (**PH2**). Through logging (**MO2**), alarms will be sent to the central system on tampering. The CPO can the detect and respond to them (**OR2**).

The impact of a physical attack is limited to one charging station (**SO-PI1**), so that the risk of more advanced physical attacks is also mitigated. Also, highly sensitive financial information, such as credit or debit card information, used for transaction authorization in encrypted end-to-end from the payment terminal to the payment company (**SO-CM3**). So, attackers cannot access it through a physical attack on the charging station.

3.3.4 Protecting against data modification or disclosure on the WAN

Communication on the WAN should be protected as often wireless and public networks are used. So, the security of the network itself cannot be trusted. Cryptographic encryption and authentication provide an effective means to protect against disclosure and modification (**CM1**).

3.3.5 Protecting against a network denial-of-service attack on the WAN interface

To protect against network denial-of-service (DoS) attacks, the charging station protects ongoing transactions against attacks on the WAN (**CM2**). Communication with the CSMS cannot reliably be protected, as the DoS may also affect the network connection. But is should be possible for authorized EV drivers to complete their transaction and finish charging. In this way, the impact of the attack to customer is reduced.

3.3.6 Protecting against an exploit of a software vulnerability

To reduce the risk of exploits of software vulnerabilities, the likelihood of vulnerabilities on the devices can be reduced by hardening (**MA3**) and by having a secure development process at the device's supplier (**SC3**).

If such vulnerabilities are discovered, CPOs can apply security updates to the charging quickly through automated management (**OR4**, **MA3**). And if vulnerabilities are present on the device, enabling security features during hardening (**MA3**) makes them harder to exploit.

3.3.7 Protecting against firmware modification

The firmware can be modified either at the developer or in transit between the developer and the charging station. To counter the first threat, the developers must protect their assets (**SC2**). To counter the second threat, the remote firmware update must protect the firmware with a digital signature (**MA3**).

Moreover, changes to the firmware are logged and can be sent to the central system (**MO2**), so that operators can detect unauthorized modifications (**OR2**).

3.3.8 Protecting against harmful actions by engineers

The main measure to prevent harmful actions by engineers are organizational security controls, such as screening and training (**OR1**), as harmful actions by authorized engineers are hard to prevent by technical measures. Logging on the charging station can help charge point operators to detect and respond to intentional or unintentional incidents caused by engineers (**MO2**).

3.3.9 Protecting against loss of stored data

The main measure to protect availability of the stored configuration is to store them securely in the central systems (**OR5**). For this approach to work, it must be possible to restore the charging station from the configuration file. No manual configuration should be needed afterwards (**MA3**).

3.4 Rationale for the baseline security requirements

Table 3 provides a mapping from the security objectives for the charging station in Section 3.1 to the baseline security requirements in Section 4, showing that a device that fulfills all the security requirements also meets the security objectives.

Table 3: Mapping of the security objectives for the device to the baseline security requirements.

Security objective	**Security requirements**
AC4 Role separation for EV drivers, engineers, CSMS, and electric vehicles	• C9.2.3 Least privileges with separate roles for EV drivers, engineers, CSMS, electric vehicles, other charging stations, and local EMS • C.9.4.2 Authentication by role for EV drivers, engineers, CSMS, electric vehicles, other charging stations, and local EMS • C10.1.1 Strong cryptographic keys and algorithms
PH2 Protection against moderate physical attacks (SL-2)	• C.11.2.2 Disabling unused hardware interfaces through OTP or muxing • C.11.2.3 Disabling debug ports • C11.2.10 Active tamper detection
CM1 Cryptographic protection of communication confidentiality and integrity on WAN	• C10.1.1 Strong cryptographic keys and algorithms • C.13.1.1 Confidentiality and integrity of network communication
CM2 Resilience of charging transactions against denial-of-service attacks on the WAN interface	• C.13.1.2 Resilience against denial-of-service attacks • C.13.1.3 Shielding charging transactions from denial-of-service attacks on the WAN
MA3 Automated management	• C10.1.1 Strong cryptographic keys and algorithms • C.10.1.4 Automated key management • C.12.1.1 Future-proof design • C.12.1.2 Zero-touch deployment • C.12.2.2 Use of platform security features

Security objective	Security requirements
	• C.12.3.3 Automated configuration management • C.12.5.2 Remote firmware updates • C.12.5.3 Verification of firmware signatures before installation • C.12.6.2 Hardened by default • C.14.2.5 Secure initial configuration
MO2 Collecting security events from the central system	• C.12.4.2 Security events • C.12.4.4 Protecting security logs • C.12.4.5 Collecting security events
SC2 Protection of assets at developer against advanced threats	• C.15.2.2 Protection of customer assets
SC3 Secure development	• C.14.2.1 Secure programming practices • C.14.2.2 Security testing during development • C.14.2.3 Support for third party testing • C.14.2.6 Vulnerability handling

4 Baseline security requirements

This section contains a set of baseline security requirements that every charging station should meet. The baseline covers security measures that most charging station vendors have implemented and that mitigate the risk that most Charge Point Operators (CPO) find in their charging facilities.

4.1 Access control

Access control requirements concern how access rights are managed and how strong the authentication needs to be for different user groups in Table 1 of Section 2.2.

4.1.1 User access management [A.9.2]

The charging station manages access rights in such a way that the CPO can implement the principle of least privileges for all the users.

C9.2.3 Least privileges with separate roles for EV drivers, engineers, CSMS, and electric vehicles

The device shall allow to enforce access control with separate roles for EV drivers, engineers, CSMS, and electric vehicles, so that they can access only the functions and data they need for their role.

Remarks: The requirement can be met by having a different user account for each role. Each account should then have its own password or keys for authentication. The requirement can also be met by full role-based access control.

4.1.2 System and application access control [A.9.4]

The charging station implements authentication for all users. For the CSMS and electric vehicles (if needed), it uses machine-to-machine authentication. For engineers, it uses passwords. For EV drivers, the authentication mechanism is determined by the mobility service provider.

C.9.4.2 Authentication by role for EV drivers, engineers, CSMS, and electric vehicles

The device shall support mutual authentication for EV drivers, engineers, CSMS, and electric vehicles with passwords or keys shared between users in the same role, so that:

- the different users can check a connection comes from a unique device, and
- the device can check that a connection comes from a unique user

Remark: In OCPP 2.0 [7] or OCPP 1.6 [8] with the security whitepaper [9], the charging station can authenticate the CSMS by using the TLS with Basic Authentication or TLS with Client-Side Authentication security profile.

4.2 Cryptography

4.2.1 Cryptographic controls [A.10.1]

The charging station uses strong cryptographic keys and algorithms to protect against attacks to the cryptography itself. The charging station supports remote key updates from the central systems to update keys on possibly hundreds of charging stations.

C10.1.1 Strong cryptographic keys and algorithms

For security functions, the charging station shall use cryptography according to regulations and modern guidelines without any modifications. In particular:

- It only uses the cryptographic algorithms that the ECRYPT – Algorithms, Key Size, and Protocols Report [10] recommends as suitable for new or future systems.
- It uses keys as least as long as the ECRYPT report recommends for near term use (section 4.6 in [10]).
- It only uses a dedicated cryptographic pseudo-random number generator meeting the requirements in the ECRYPT report [10] Section 3.2.3 to generate random numbers for security functions.
- If it uses certificates for authentication, it validates them by checking the signature, the certificate-chain, the revocation status, and the identity or role of the user.

Remark: The requirement applies for instance for the cryptography used in:

- machine-to-machine authentication (C.9.4.2)
- hashing passwords used by human users (C.9.4.4)
- digitally signing the firmware (C.12.5.3)
- protecting the confidentiality and integrity of communication (C.13.1.1)

When validating a certificate, the identity of the user can be checked through the subject name, common name, or distinguished name.

The algorithms and key lengths in OCPP 2.0 or OCPP 1.6 with the security whitepaper met the requirement.

C.10.1.4 Automated key management

The charging station shall support automated key management by:

- being delivered with unique initial keys installed during manufacturing.
- allowing all keys to be remotely updated in such a way that their confidentiality and integrity is cryptographically protected during transport.

If asymmetric cryptography is used to protect communication, the device shall be able to use certificates given out by the charge point operator’s public key infrastructure (PKI).

The device shall support remotely changing all passwords in a way that protects their confidentiality and integrity.

Remarks: OCPP 2.0 or OCPP 1.6 with the security whitepaper include use cases to update all keys and passwords used in the protocol. See Appendix B.

It is allowed that some passwords or keys used for internal purposes cannot be updated remotely. But as soon as they are used to implement any of the requirements in this document, the requirement applies.

Public keys or certificates used to verify firmware signatures may come from an external PKI used by the vendor. It is not required that the device can use certificates from the charge point operator’s PKI for this purpose.

4.3 Physical and environmental security

4.3.1 Equipment [A.11.2]

The charging station is protected against moderate physical attacks by disabling unused ports and interfaces and detecting tampering of the device.

C.11.2.2 Disabling unused hardware interfaces through OTP or muxing

The device shall disable unused hardware interfaces by:

- configuring it in One-time-programmable (OTP) memory, or E-fuses.
- muxing the pins during early boot

Remark: One-time-programmable memory (OTP) cannot be changed once the content is programmed. Unused hardware interfaces can be permanently closed by configuring it in the fuses of OTP memory or E-fuses. Another way to disable hardware interfaces is by controlling (disabling) the physical connections from the unused interfaces to the pins through multiplexing.

C.11.2.3 Disabling debug ports

The device shall restrict access to its debug ports by either:

- fully closing the debug ports using fuses in One-Time-Programmable (OTP) memory or e-fuses, or
- password protecting the debug ports

C.11.2.10 Active tamper detection

The device shall allow physical tampering to be detected by:

- having a cover that protects against physical manipulation, so that attackers without specialist tools cannot reach its internals without leaving visible traces;
- creating a log event and sending an alert whenever any part of its cover is opened.

4.4 Operations security

The charging station should support the operational processes and procedures needed to keep it secure throughout its lifetime.

4.4.1 Operational procedures and responsibilities [A.12.1]

To support capacity management, the charging station needs to have enough computing reserves for future updates.

C.12.1.1 Future-proof design

The device shall have enough memory (RAM and flash) and computation power to allow security updates needed during its lifetime, under the following assumptions:

- Cryptographic measures are updated following the standards in C.10.1.1, in particular, the device supports the key sizes recommended for long term use in Section 4.6 of the ECRYPT report [10];
- Roles and security event types will grow incrementally up to 50%.

Remarks: Compliance with the requirement can be shown through performance tests. Tests with current firmware under operational workloads should show that there are enough reserves to extend security functions. Tests with algorithms recommended for long-term use in [10] should show that the device can run them without affecting operations. It is acceptable if the device can only support the long-term key sizes for elliptic curve-based algorithms, not for RSA-based algorithms.

C.12.1.2 Zero-touch deployment

The device shall support zero-touch deployment: it can be installed without local access, through the following steps.

- The vendor delivers the device to the charge point operator with an initial configuration, passwords, and keys installed.
- Once the device has been physically installed and is powered, it automatically connects to a commissioning server.
- The commissioning server loads the operational configuration to the device, including new passwords and keys

4.4.2 Protection from malware [A.12.2]

The charging station is protected against exploits and malware by using available platform security features.

C.12.2.2 Use of platform security features

The device shall use security features from the underlying hardware and software platform whenever possible.

Remark: It is recommended to use the following hardware features when they are supported:

- *No-Execute (NX) / Write-xor-execute (W^R):* A Memory Protection Unit (MPU) or Memory Management Unit (MMU) shall be used to mark code regions as read-only and data sections as non-executable.
- *Address Space Layout Randomization (ASLR):* A Memory Management Unit (MMU) shall be used to load data and code at different memory addresses every time an application is run.
- The software running on the device must be compiled to use the hardware features. The Position Independent Code (PIC) or Position Independent Executable (PIE) compiler options should be enabled to be able to use ASLR.

4.4.3 Backup [A.12.3]

To support recovery processes, it should be possible to recover the charging station from the backups stored in the CSMS.

C.12.3.3 Automated configuration management

The device shall allow the central system to change and monitor its configuration.

Remarks: As the CSMS keeps all device configurations, these are automatically backed up when back-ups of the servers are made. No separate back-up process is needed for the charging stations.

4.4.4 Logging and monitoring [A.12.4]

To support detecting and responding to security incidents, the charging station needs to log relevant security events and allow them to be gathered for analysis. As the security logs are important to security, they also need to be protected themselves.

C.12.4.2 Security events

The device shall be able to store in a local log all events relevant to its security, such as:

- Successful authentications
- Failed authentication attempts
- Firmware uploads
- Successful firmware updates
- Failed firmware updates
- Changing the device configuration
- Changing the system time
- Booting the device
- Shutting down the device
- Changing keys or credentials
- Failed attempt to change keys or credentials
- Changing user accounts
- Changing authorizations

The log entries for security events shall include a timestamp, an event description, and the role causing the event. Events caused by engineers are linked to individual users.

Remark: The security events are implemented in OCPP 2.0 or OCPP 1.6 with the security whitepaper. See Appendix B.

C.12.4.4 Protecting security logs

The device shall protect security logs by:

- restricting access to authorized users
- having enough storage capacity to store the security logs
- implementing a rolling security log, in which the oldest entries are discarded first if log storage is full

Remark: Normally only the system and root users should be allowed to modify the logs, and only specific user groups should be authorized to read them.

C.12.4.5 Collecting security events

The device shall allow the security logs to be read out using the normal maintenance tools and shall be able to send all security logs to the CSMS.

The device shall provide the capability to create timestamps that are synchronized with a system-wide time source.

Remark: in OCPP 2.0 or OCPP 1.6 with the security whitepaper, the critical security events are sent to the CSMS as notifications. The CSMS can gather other events by reading the logs. See Appendix B.

4.4.5 Control of operational software [A.12.5]

The authenticity of firmware updates is verified using a digital signature.

C.12.5.2 Remote firmware updates

The device shall allow remote software or firmware updates from the central system for all security functionality for which updates are expected to be needed. In particular, the device shall allow to remotely:

- update all cryptographic algorithms and protocols
- update the cryptographic random number generator
- add more roles
- change the authorization of role

Remark: Remote firmware updates are part of OCPP 2.0 or OCPP 1.6 with the security whitepaper. See Appendix B.

C.12.5.3 Verification of firmware signatures before installation

The device shall be able to verify the authenticity of firmware updates using digital signatures before installing the firmware. The vendor digitally signs each firmware release.

Remark: Verifying the firmware signature is part of the firmware update process in OCPP 2.0 or OCPP 1.6 with the security whitepaper. See Appendix B.

Verifying the firmware integrity using only a hash value does not satisfy the requirement. It is recommended to also encrypt the firmware during transport, to make it harder to reverse engineer it and find vulnerabilities.

4.4.6 Technical vulnerability management [A.12.6]

To support effective vulnerability management, the charging station is hardened by disabling unneeded functions and enabling security features.

C.12.6.2 Hardened by default

The device shall be delivered with all unneeded functions disabled. In particular, it shall be delivered with:

- all unused user accounts removed
- all unused network services disabled
- all unused hardware interfaces disabled

The device shall be delivered with the security features from the underlying hardware and operating system enabled whenever possible.

Remarks: It is recommended to disable hardware ports in software and to remove traces, pins and components from the PCB.

If a VPN tunnel is used, the device must allow closing all services not used outside of the tunnel.

4.5 Communication security

4.5.1 Network security management [A.13.1]

The charging station needs to support securing communications on the WAN network.

C.13.1.1 Confidentiality and integrity of network communication

The device shall be able to cryptographically protect the integrity and confidentiality of communication on the WAN interface. The measures shall allow to verify the source of messages and protect against replay and man-in-the-middle attacks.

Remark: Confidentiality and integrity of the communication can be protected by using the TLS with Basic Authentication or TLS with Client-Side authentication security profile in OCPP 2.0 or OCPP 1.6 with the security whitepaper.

C.13.1.2 Resilience against denial-of-service attacks

The device shall be resilient against denial-of-service attacks. It shall not become unavailable for long times when network interfaces are flooded with data, or when malformed messages are sent on network interfaces.

Remarks: The device may become slower when flooded or when dealing with malformed packets. But it should not crash or reboot so that it is not reachable for a longer time.

C.13.1.3 Shielding charging transactions from denial-of-service attacks on the WAN

The device shall ensure that charging transactions keep working normally when the WAN interface is flooded with data or receives malformed messages.

4.6 System acquisition, development, and maintenance

4.6.1 Security in development and support processes [A.14.2]

The developer should integrate security throughout their development process to ensure that secure firmware is delivered. They should set up secure programming practices and test each firmware release themselves. They should allow the CPO to verify the security by acceptance testing as well as provide guidelines on secure configuration and operation. If vulnerabilities are found during the lifetime of the device, they should provide security updates.

C.14.2.1 Secure programming practices

The developer shall set up programming practices for the device firmware. They shall:

- define secure coding guidelines
- provide security training to developers
- set up internal code reviews
- use an issue tracker to follow the vulnerabilities and other security issues
- implement a version control system
- enable compiler options to harden binaries or use memory-safe languages

Remark: Examples of secure coding guidelines are the SEI CERT coding standards [11], available for different languages, and the MISRA C software development guidelines for embedded systems [12].

Compiler options that should be enabled include:

- stack cookies or canaries which make it harder to exploit stack-based buffer overflows
- fortify source which can be used to detect buffer overflow vulnerabilities
- Control Flow Integrity (CFI) which makes it harder for an attacker to perform code re-use attacks such as return-to-libc or Return Oriented Programming (ROP)

C.14.2.2 Security testing during development

The developer shall test each firmware release to find vulnerabilities and check the implementation of the requirements in this document. Testing shall at least include:

- functional testing for all functional requirements
- robustness testing of custom protocol implementations
- automated web application testing on any web interfaces
- automated vulnerability scanning

The developer shall make the results of these tests available to the charge point operator on request.

Remarks: The device developer should test that their code checks the validity of all input data, including validating if values are within the permitted value range. They should monitor for input validation vulnerabilities in third-party libraries or applications. They should also use reviews and robustness tests for code they develop in-house, such as web interfaces or the implementation of domain-specific protocols such as IEC 104. For web services, it is recommended to follow the recommendations from the Open Web Application Security Project (OWASP) [13] [14].

C.14.2.3 Support for third party testing

The developer shall support testing by the charge point operator or an independent party by:

- allowing the charge point operator or a third party to audit the development process
- providing documentation on how the requirements have been implemented
- making available devices for testing
- providing all keys and credentials needed for testing
- providing access to source code for code reviews

Remark: The developer may require a non-disclosure agreement when providing sensitive information as long as it does not prevent proper testing.

C.14.2.5 Secure initial configuration

The developer shall deliver the device with a secure initial configuration:

- access control and communication security measures are turned on
- unique initial keys and passwords are installed
- security alarms are sent to the central system
- the sensors are hardened

C.14.2.6 Vulnerability handling

The developer shall produce security updates to fix all severe vulnerabilities found during the lifetime of the device. The developer shall monitor all relevant information sources on vulnerabilities, including:

- public vulnerability databases
- notifications from developers of libraries used in the firmware
- penetration test results from customers
- notifications from vulnerability researchers

The developer shall inform the charge point operator about vulnerabilities as soon as possible.

Remark: As vulnerabilities should be considered at least:

- vulnerabilities for third party libraries and applications reported in public databases, such as the Common Vulnerabilities and Exposures (CVE) database
- issues that would allow bypassing the security measures in this document
- input validation issues
- denial-of-service issues that can be exploited remotely
- failures of security measures due to hardware malfunctions, corruption of stored or received data and software crashes

To determine which vulnerabilities are severe, the Common Vulnerability Scoring System (CVSS) can be used. Vulnerabilities with a score of 7.0 or higher would be considered severe and need to be fixed. The developer may agree with the charge point operator to use another method to determine the severity of the vulnerabilities if it can be objectively applied and gives a good indication of the risk.

4.7 Supplier relationships

4.7.1 Information security in supplier relationships [A.15.2]

To ensure that the developer protects the information of the charge point operator (CPO) or under his responsibility, it needs to implement an information security management system (ISMS).

C.15.2.2 Protection of customer assets

The developer shall have an ISO/IEC 27001 certified ISMS that protects the confidentiality, integrity, and availability of any assets that could compromise the security of the device, including:

- detailed security designs
- source code
- the development and build environment
- private keys used for firmware signing
- customer-specific keys and credentials

Remark: The certification scope should cover the development and manufacturing of the device and related tools.

Appendix A: Mapping to IEC 62443

The tables below map the security objectives for the charging station in Section 3.1 to the requirements in IEC 62443-4-2 [5] and IEC 62443-4-1 [15]. If a product satisfies the requirements as specified in the tables, then it also meets the security objectives. Only the IEC 62443 requirements needed to meet the objectives are included in the tables.

The table in Appendix A.3 includes a series of extensions to IEC 62443-4-1 and IEC 62443-4-2 that are needed to fully cover the objectives.

The IEC 62443 requirements have been chosen to be as close to the baseline security requirements in Section 4 as possible. But it is not possible to make the requirements exactly equivalent at this level of detail.

A.1 Mapping to IEC 62443-4-1

The table below lists the requirements selected from the IEC 62443-4-1 [15] standard on *Secure product development lifecycle requirements* to meet the security objectives. We would recommend developers to also consider the requirements not included in the table, as these can further improve security in development processes. The IEC 62443-4-1 requirements correspond to the baseline security requirements for *System acquisition, development, and maintenance requirements* (Section 4.6), and *Supplier relationship requirements* (Section 4.7).

IEC	Name	Obj
SM-1	Development process	SC3
SM-2	Identification of responsibilities	SC3
SM-4	Security expertise	SC3
SM-6	File integrity	SC2
SM-7	Development environment security	SC2
SM-8	Controls for private keys	SC2
SM-9	Security requirements for externally provided components	SC3

IEC	Name	Obj
SM-10	Custom developed components from third-party suppliers	SC3
SM-11	Assessing and addressing security-related issues	SC3
SM-12	Process verification	SC3
SM-13	Continuous improvement	SC3
SI-1	Security implementation review	SC3
SI-2	Secure coding standards	SC3
SVV-1	Security requirements testing	SC3
SVV-2	Threat mitigation testing	SC3
SVV-3	Vulnerability testing	SC3
SVV-4	Penetration testing	SC3
DM-1	Receiving notifications of security-related issues	SC3
DM-2	Reviewing security-related issues	SC3
DM-3	Assessing security-related issues	SC3
DM-4	Addressing security-related issues	SC3
DM-5	Disclosing security-related issues	SC3
SUM-4	Security update delivery	SC3
SG-1	Product defense in depth	MA3

IEC	Name	Obj
SG-2	Defense in depth measures expected in the environment	MA3
SG-3	Security hardening guidelines	MA3
SG-5	Secure operation guidelines	MA3
SG-6	Account management guidelines	AC4

A.2 Mapping to IEC 62443-4-2

The table below lists the requirements selected from the IEC 62443-4-2 standard on *Technical security requirements for IACS components* [5]. We are using the embedded device requirement (EDR) from IEC 62443-4-2.

IEC	Name	Obj
CR1.1	Human user identification and authentication	AC4
CR1.2	Software process and device identification and authentication	AC4
CR1.3	Account management	AC4
CR1.5	Authenticator management	MA3
CR1.8	Public key infrastructure certificates	MA3
CR1.9	Strength of public key-based authentication	AC4 CM1 MA3
CR2.1	Authorization enforcement	AC4

IEC	Name	Obj
CR2.1 RE1	Authorization enforcement for all users (humans, software processes and devices)	AC4
CR2.6	Remote session termination	AC4
CR2.8	Auditable events	MO2
CR2.9	Audit storage capacity	MO2
CR2.10	Response to audit process failures	MO2
CR2.11	Timestamps	MO2
CR2.11 RE1	Time synchronization	MO2
CR2.11 RE2	Protection of time source integrity	CM1
CR3.1	Communication integrity	CM1
CR3.1 RE1	Communication authentication	CM1
CR3.8	Session integrity	CM1
CR3.9	Protection of audit information	MO2
CR4.1	Information confidentiality	CM1
CR4.3	Use of cryptography	AC4 CM1 MA3
CR6.1	Audit log accessibility	MO2

IEC	Name	Obj
CR6.1 RE1	Programmatic access to audit logs	MO2
CR7.1	Denial-of-service protection	CM2
CR7.3	Control system backup	MA3
CR7.4	Control system recovery and reconstitution	MA3
CR7.7	Least functionality	MA3 PH2
EDR2.13	Use of physical diagnostic and test interfaces	PH2
EDR3.2	Protection from malicious code	MA3
EDR3.10	Support for updates	MA3
EDR3.10 RE1	Update authenticity and integrity	MA3
EDR3.11	Physical tamper resistance and detection	PH2
EDR3.11 RE1	Notification of a tampering attempt	PH2
EDR3.12	Provisioning product supplier roots of trust	MA3
EDR3.13	Provisioning asset owner roots of trust	MA3

A.3 Extensions to IEC 62443

The following extensions to the IEC 62443 requirements are needed to fully cover the security objectives.

Name	Description	Obj
	Extensions to IEC 62443-4-1	
SVV-1 EE1: Support for third party testing	The developer shall support testing by the charge point operator or an independent party	SC3
SM-7 EE2: Certified information security management	The developer shall have an ISO/IEC 27001 certified information security management system (ISMS) that protects any information that could compromise the security of the device, including: • detailed security designs • source code • customer-specific keys and credentials *Remarks:* The certification scope should cover the development and manufacturing of the device and related tools.	SC2
	Extensions to IEC 62443-4-2	
CR1.1 EE1: Role identification for human users	Components shall be able to identify the role of [users].	AC4
CR1.2 EE1: Mutual identification and authentication for software processes and devices	Components shall provide the capability to identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the components to support least privilege in accordance with applicable security policies and procedures.	AC4
CR1.2 EE2: Mutual identification and authentication for software processes and devices based on network location	Components shall provide the capability to provide authentication for [users] through one of the following options : A. Based on their network location through a VPN terminating at the device. Mutual authentication shall be	AC4

Name	Description	Obj
	used between the device and a network device (e.g. firewall or concentrator) at the central system during the setup of the VPN. Unique passwords or keys can be used for each device. B. Using unique mutual authentication, so that the [users] can check that a connection comes from a unique device, and the device can check that a connection comes from a unique [users]	
CR1.5 EE2: Remote authenticator update	Components shall provide the capability to update all authenticators.	MA3
CR1.5 EE3: Unique initial authenticator	Components shall be delivered with unique initial authenticators for the device during manufacturing.	MA3
CR2.1 EE1: Role separation	Components shall provide the capability to set different authorizations for different roles, allowing to define at least roles for [users].	AC4
CR4.3 EE1: Use of cryptography according to ECRYPT recommendations	Components shall follow the recommendations in the ECRYPT – Algorithms, Key Size, and Protocols Report [8]. In particular: ○ It only uses the cryptographic algorithms that the ECRYPT recommends as suitable for new or future systems. ○ It uses keys as least as long as the ECRYPT report recommends for near term use (section 4.6 in the ECRYPT report). ○ It only uses a dedicated cryptographic pseudo-random number generator meeting the requirements in the ECRYPT	AC4 CM1 MA3

Name	Description	Obj
	report (Section 3.2.3) to generate random numbers for security functions.	
CR7.7 EE1 Disable unused hardware ports through OTP or muxing	Components shall provide the capability to disable all unused hardware ports through one-time programmable memory (OTP) or muxing.	PH2
EDR3.10 EE1: Update capacity	Components shall have enough memory (RAM and flash) and computation power to allow security updates needed during its lifetime.	MA3
EDR3.10 EE2: Remote updates	Components shall allow the updates to be performed remotely from a centralized system.	MA3
CR7.7 EE1: Hardening by default	The device shall be delivered with all unneeded functions disabled. In particular, it shall be delivered with: • all unused user accounts removed • all unused network services disabled • all unused hardware interfaces disabled The device shall be delivered with the security features from the underlying hardware and operating system enabled whenever possible.	MA3

A.4 Rationale

Below a rationale is provided for the requirements selected in A.1, A.2, and A.3 by showing that they cover the security objectives for the charging station in Section 3.1.

AC4 Role separation for the EV drivers, engineers, CSMS, and electric vehicles

Authentication is covered by requirement *CR1.1* and *CR1.2* with the extensions *CR1.1 EE1* and *CR1.2 EE1* to ensure mutual authentication. Strong cryptographic keys and algorithms for the authentication are ensured by requirements *CR1.9* and *CR4.3* with the extension *CR4.3 EE1*. Remote session termination (CR2.6) is included to reduce the risk that authentication is bypassed by compromising a session.

Authorization is covered by *CR2.1* and *CR2.1 RE1* with the extension *CR2.1 EE1* to ensure that roles can be separated. Account management (*CR1.3*) is required to manage the account of different roles. Requirement *SG-6* ensures that the developer provides guidelines for account management.

PH2 Protection against moderate physical attacks (SL-2)

Physical attacks are prevented on the outside by disabling unused hardware port as part of requirement *CR 7.7*. To ensure the ports are not enabled during boot or other unusual software states, the ports should be disabled using one-time programmable memory (OTP) or muxing (*CR 7.7 EE2*).

The insides of the device should be protected by physical tamper resistance and detection (*EDR 3.11*) and by disabling diagnostic and test interfaces (*EDR 2.13*).

Requirement *EDR 3.11 RE1* ensures that an alarm is sent to the CSMS when someone tries to physically access it.

Together the measures can mitigate the risks of physical attacks by attackers with moderate skills and resources.

CM1 Cryptographic protection of communication confidentiality and integrity on WAN

Protecting the confidentiality of the information is covered by requirement *CR4.1*. Integrity of the communication by *CR3.1*, *CR3.1 RE1*, and *CR 3.8*. Requirements *CR 1.9*, *CR4.3*, and *CR 4.3 EE1* ensure that strong cryptography is used to protect the communication.

CM2 Resilience of charging transactions against denial-of-service attacks on the WAN interface

Resilience against denial-of-service attacks is provided by requirement *CR7.1*. The essential functions in this case are the charging transactions.

MA3 Automated management

Automated updates of keys and credentials are covered by requirement *CR1.5* with the extension *CR1.5 EE2*. The extension *CR1.5 EE3* ensures that the charging station is delivered with unique keys and credentials installed. Requirement *EDR 3.13* allows a root certificate from the charge point operator to be installed, so that it can be integrated in their PKI.

Updates of software and firmware are covered by *EDR 3.10*. The extension *EDR 3.10 EE2* ensures that the updates can be performed remotely, while *EDR 3.10 EE1* ensures there is enough memory and computing power for future updates. The authenticity of the software and firmware is protected by digital signatures according to requirement *EDR 3.10 RE1*. Requirement *CR1.8* ensures that the device can be integrated into a PKI for the certificates needed to verify the signature. Requirements *CR1.9*, *CR4.3*, and *CR4.2 EE1* ensure the strength of the cryptography used for the signatures.

Restoration from a backed-up configuration is covered by requirements *CR 7.3* and *CR 7.4*.

Disabling unneeded functions is covered by requirement *CR 7.7*, enabling security features of the platform by *EDR 3.2*. The extension *CR7.7* ensures that the device is delivered in a secure state. Requirements *SG-1*, *SG-2*, *SG-3, and SG-5* ensure the developer provides security guidelines for hardening the device.

MO2 Alerting security events to central systems

Requirement *CR2.8* ensures that security events are logged, while requirements *CR6.1* and *CR6.1 RE1* ensure that they can be sent to a centralized system, in this case the CSMS.

Protection of the security logs is covered by requirements *CR2.10* and *CR3.9*. Requirement *CR2.9* ensures that there is enough storage capacity on the device for the logs.

Time synchronization is covered by requirements *CR2.11* and *CR2.11 RE1*. Requirement *CR2.11 RE2* ensures that the integrity of the time source is protected.

SC2 Protection of assets at the developer against advanced threats

Protection of assets at the developer is covered by requirement *SM-6*, *SM-7*, and *SM-8*. The extension *SM-7 EE2* ensures the assets are protected by a certified ISMS.

SC3 Secure development

Secure programming practices are covered by requirements *SM-1*, *SM-2*, *SM-12* and *SM-13*. Requirements *SM-9* and *SM-10* are needed to ensure the processes also cover third-party suppliers. Requirement *SM-4* ensures that the developer has the security expertise need for the processes. Secure programming practices are covered by *SI-1* and *SI-2*. Security testing during development is covered by requirements *SM-11*, *SVV-1*, *SVV-2*, *SVV-3*, and *SVV-4*. The extension *SVV-1 EE1* is included to allow charge point operators to perform their own testing. The delivery of secure updates is covered by SUM-4. Vulnerability handling is covered by the requirements *DM-1*, *DM-2*, *DM-3*, *DM-4*, and *DM-5*.

Appendix B: Implementing the requirements in OCPP 2.0

This appendix explains how many of the requirements can be met by implementing the OCPP 2.0 standard [7] or OCPP 1.6 [8] with the security whitepaper [9] used by many charging stations.

B.1 Requirements fully covered by OCPP 2.0

The requirements in Table 4 can be fully implemented by following the OCPP 2.0 standard. If the charging station is compliant with OCPP 2.0, it automatically meets these security requirements.

Table 4: Requirements fully covered by OCPP 2.0.

Requirement	**Section in [7]**	**OCPP Implementation**
C.12.4.2 Alerting security events to the central system	Enumeration 2.73	The events in enumeration 2.73 are logged.
C.12.5.2 Remote firmware updates	L. Firmware management	OCPP 2.0 defines use cases for remotely updating the firmware.
C.12.5.3 Verification of firmware signatures before installation	L.2.L02	The secure firmware update process defined in OCPP 2.0 use case L02 uses digital signatures. Note that to meet the requirement, non-secure firmware updates (use case L03) should be disabled.

B.2 Requirements partially covered by OCPP 2.0

The requirements in Table 5 are covered by the OCPP 2.0 as far as they concern the security functions of the OCPP protocol. For security functions not part of the OCPP standard, these requirements need to be implemented independently from the OCPP 2.0 standard.

Table 5: Requirements partially covered by OCPP 2.0.

Requirement	Section in [7]	OCPP Implementation
C.9.2.3 Least privileges with separate roles for the CSMS, EV drivers, electric vehicles, other charging stations, and the local EMS	-	The OCPP protocol implicitly defines the access rights of the CSMS by describing which functions are exposed over OCPP.
C.9.4.2 Authentication by role for EV drivers, engineers, CSMS, electric vehicles, other charging stations and the local EMS (for CSMS)	A.1.3.4 – A.1.3.7	OCPP 2.0 offers two profiles. In both profiles the CSMS authenticates using a TLS and a certificate. With the TLS with Basic Authentication profile, the charging station authenticates using HTTP basic authentication and a password. With the TLS with Client-Side Certificates profile, the charging station authenticates using TLS and a client-side certificate.
C.10.1.1 Strong cryptographic keys and algorithms	A.1.3.5, A.1.3.7 A.1.4.1 L.2.L01	OCPP 2.0 defines algorithms and keys lengths for all cryptographic mechanisms it uses.
C.10.1.4 Automated key management	A.2.A01, A.2.A02, A.2.A03, M.2.M05, M2.M06	The passwords and keys that the charging station uses to authenticate to the CMSM can be updated through use cases A01 - A03. All CA certificates can be updated through use cases M05 and M06.
C12.4.5: Collecting security events	Appendix 1, A.2.A04, N.2.N01	For events that are defined as critical in Appendix 1, a notification is sent to the CSMS through use case A04. Logs for other events can be retrieved through the normal logging mechanism (use case N01). Retrieving logs locally is out of scope for OCPP.

C.13.1.1 Confidentiality and integrity of network communication	A.1.3.4 – A.1.3.7	In both the TLS with Basic Authentication and TLS with Client-Side authentication, the confidentiality and integrity of the communication is protected through TLS.

B.3 Requirements not covered by OCPP 2.0

The following requirements are not covered by OCPP 2.0, and should be implemented separately:

- C.11.2.2 Disabling unused hardware interfaces through OTP or muxing
- C.11.2.3 Disabling debug ports
- C.11.2.10 Active tamper detection
- C.12.1.1 Future-proof design
- C.12.1.2 Zero-touch deployment
- C.12.2.2 Use of platform security features
- C.12.3.3 Automated configuration management
- C.12.6.2 Hardened by default
- C.13.1.2 Resilience against denial-of-service attacks
- C.13.1.3 Shielding charging transactions from denial-of-service attacks on the WAN
- C.14.2.1 Secure programing practices
- C.14.2.2 Security testing during development
- C.14.2.3 Support for third party testing
- C.14.2.5 Secure initial configuration
- C.14.2.6 Vulnerability handling
- C.15.2.2 Protection of customer assets

Glossary

APN	Access Point Name
CPO	Charge Point Operator
CSMS	Charging Station Management System
CVSS	Common Vulnerability Scoring System
DoS	Denial-of-Service
EMS	Energy Management System
EV	Electric Vehicles
ISMS	Information Security Management System
OCPP	Open Charge Point Protocol
PKI	Public Key Infrastructure
SCADA	Supervisory Control And Data Acquisition
TLS	Transport Layer Security
VPN	Virtual Private Network
WAN	Wide Area Network

References

[1] SANS and E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid - Defense Use Case," 2016.

[2] ISO/IEC, "ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements," 2013.

[3] ENCS, "Security risk assessment for EV charging infrastructure," 2019.

[4] ENCS, "Security architecture for EV charging infrastructure," 2019.

[5] ISA / IEC, "ISA 62443-4-2 Security for industrial automation and control systems - Technical security requirements for IACS components, Draft 3, Edit 4," January 12 ,2017.

[6] ENCS, "Security test plan for charging stations," 2019.

[7] Open Charge Alliance, "OCPP 2.0 - Part 2 - Specification," 2018.

[8] Open Charge Alliance, "Open Charge Point Protocol 1.6," [Online]. Available: https://www.openchargealliance.org/protocols/ocpp-16/. [Accessed 2022].

[9] Open Charge Alliance, "Improved security for OCPP 1.6-J edition 2," 2020.

[10] ECRYPT - CSA, "D5.4 Algorithms, Key Size and Protocols Report," 2018.

[11] Carnegie Mellon University (CMU), "SEI CERT C Coding Standard," [Online]. Available: https://wiki.sei.cmu.edu/confluence/display/c/SEI+CERT+C+Coding+Standard. [Accessed 10 10 2019].

[12] MISRA, "Guidelines for the Use of the C Language in Critical Systems," 2013.

[13] OWASP Foundation, "OWASP Top Ten," [Online]. Available: https://owasp.org/www-project-top-ten/. [Accessed 2 12 2020].

[14] OWASP Foundation, "OWASP Web Security Testing Guide," [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/. [Accessed 2 12 2020].

[15] ISA/IEC, "IEC 62443-4-1: Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements," 2018.