EV-311-2022

Security requirements from IEC 62443 for procuring EV charging stations

Version 2022v0.1

4 January 2023

This document was produced in the ENCS program on Security Architectures. This program supports 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/resources/security-requirements/):

This document is shared under the Traffic Light Protocol classification:

TLP White – public

ENCS

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
October 2022	0.1 (2022v0.1)	Initial release of IEC62443 requirements for EV charging stations following objectives from ISO/IEC 27002:2022

Table of Contents

1 Introduction

This document gives security requirements that Charge Point Operators (CPO) can use when procuring new charging stations. The requirements are based on the IEC 62443-4-2 standard [1].

Cyber-attacks on the electric vehicle charging infrastructure are not just a financial and reputational risk to the Charge Point Operators (CPOs) that manage the infrastructure. They are also becoming a large societal risk.

Electric vehicle charging is quickly becoming an essential service to our society. As we are transitioning to electric vehicles, more and more people will rely on charging for their mobility. If the charging infrastructure is not working, people cannot use their cars. So, cyber-attacks on the infrastructure can lead to major societal damage.

Moreover, the EV charging infrastructure could be used to attack the power grid. Large CPOs remotely control hundreds of thousands of charging stations throughout Europe. If attackers gain control of a CPO's infrastructure, they could switch the power of the connected charging stations on and off. The switching could also cause grid imbalances in the supply and demand for electricity. If these imbalances are large enough, they could lead to severe power outages [2].

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 use requirements from 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.

The requirements are based on the IEC 62443 standard. They have been selected from part *IEC 62443-4-2: Technical security requirements for IACS components* [1]. This standard is widely supported by manufacturers and charge point operators, allowing the requirements to be more easily implemented.

The requirements have been designed to allow certification based on the new certification schemes being developed for IEC 62443. Together with the threat analysis for EV charging infrastructure in [4] they form a profile for IEC 62443 (following the rules in [5]). The profile also meets the requirements for a component context analysis, as defined in the JRC *Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS)* [6].

When grid operators use the technical requirements below, it is recommended to also require that the supplier complies fully to **IEC 62443-4-1** [7] **at maturity level at least 3**. Doing so, ensures that the supplier has secure development processes, so that they can correctly and consistently implement the requirements.

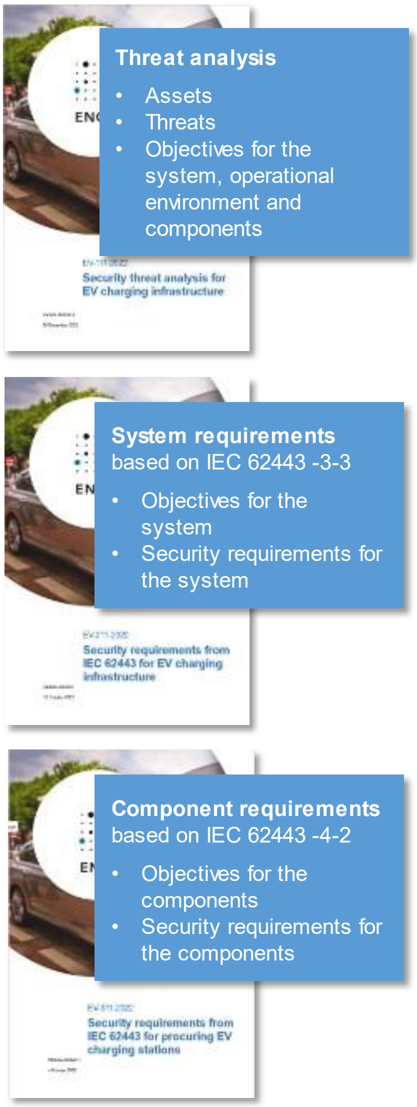
1.1 Relation to other documents

This document is part of a larger series on EV charging infrastructure security (see Figure 1). The series starts with a threat analysis [4] that determines the security objectives to counter the threats posed to the assets in a typical EV charging infrastructure. The objectives are split into objectives for the system and operational environment. The objectives for the system are the basis for the security requirements for the system in [8].

The objectives for the operational environment should be implemented by CPOs outside of the system to operate it securely. Many CPOs will meet these security objectives through their information security management system. Hence, the objectives are linked to controls from the ISO/IEC 27002:2022 standard [9]. They include organizational, people, physical, and technological objectives.

From the security objectives for the system, Section 3 derives security objectives for EV charging stations. The objectives are chosen so that a charging station meeting the component objectives can be easily integrated into a charging infrastructure meeting the system objectives. The security objectives are the basis for the requirements for EV charging stations in Section 4.

How to use the document


Security threat analysis for EV charging infrastructure
Security requirements from IEC 62443 for EV charging infrastructure
Security requirements from IEC 62443 for procuring EV charging stations

Threat analysis

- Assets
- Threats
- Objectives for the system, operational environment and components

- Check if all threats are mitigated by the security objectives or if additional objectives are needed
- Get objectives for the operational environment, to be implemented for instance through an ISMS

System requirements based on IEC 62443 -3-3

- Objectives for the system
- Security requirements for the system

- Use as requirements when procuring a complete system
- Set technical requirements to internal department maintaining the system

Component requirements based on IEC 62443 -4-2

- Objectives for the components
- Security requirements for the components

- Use as requirements when procuring components for the system

Figure 1: Relation between the different documents on EV charging infrastructure security.

2 Device description

To effectively use the security requirements, it is important to know the assumptions they make about how the EV charging station works. This includes the intended use of the device, its operational environment, and the access control mode used in the threat assessment [4] to set security objectives.

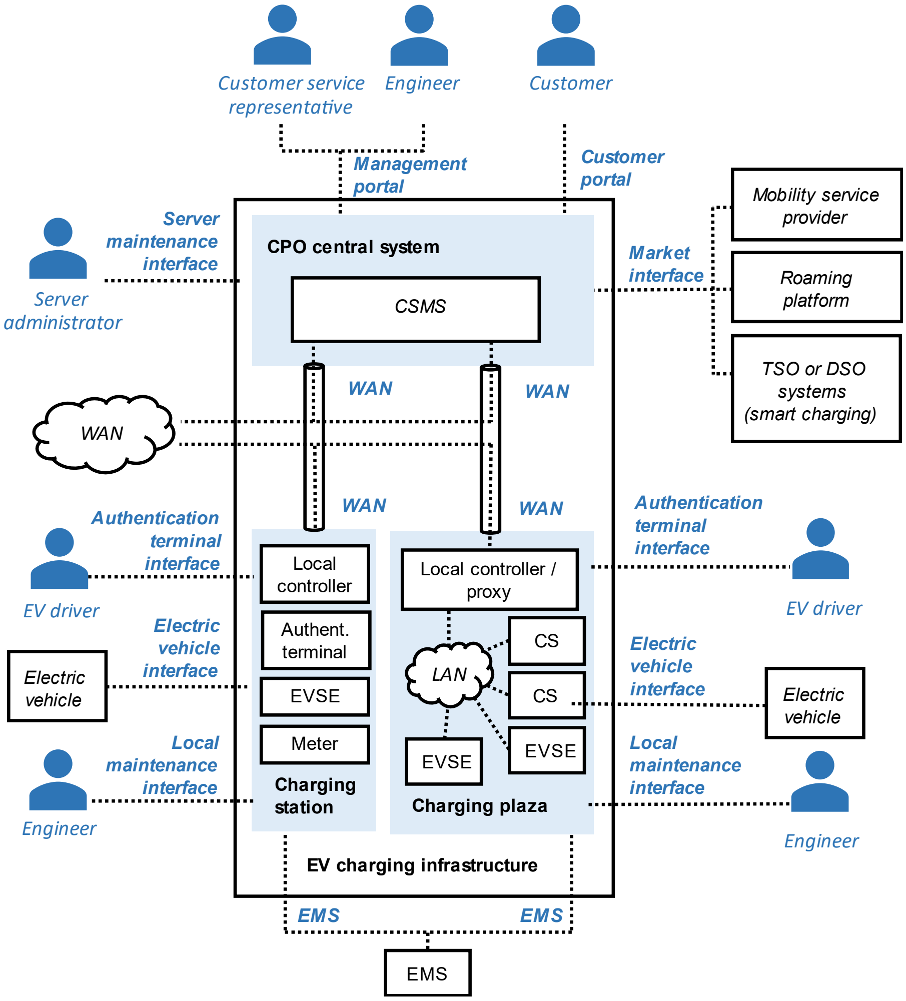


Figure 2: Reference architecture for the EV charging infrastructure, showing its users and interfaces. The requirements in this document concern the EV charging station.

2.1 Intended use of the device

This document gives requirements for procuring electrical vehicle charging stations that are controlled remotely by a Charge Point Operator (CPO). 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 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 requirements for securing 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.

2.2 Intended operational environment

The intended operational environment of the EV charging infrastructure is shown in the reference architecture (Figure 2).

2.2.1 Interfaces

The EV charging station is connected to the operational environment on the following interfaces.

2.2.1.1 WAN interface

The charging station is connected to the CPO central system over a wide-area network (WAN). The CPO central collects meter values and transaction data. The other way around, the CPO central system may send charging profiles, set tariffs, or install configurations and updates on the charging station.

The WAN is usually a wireless mobile network, such as a GPRS or LTE network. Network segregation measures such as private APNs are commonly used.

The CSMS often manages the charging stations through the Open Charge Point Protocol (OCPP). This protocol allows to change the setting, perform firmware updates, and collect logs. The reference architecture assumes that all remote maintenance is done through the CSMS central system.

2.2.1.2 Authentication terminal interface

Users authenticate to the charging station through the authentication terminal interface. Some of the most common methods include RFID cards, bank cards, authentication through an application. In the near future, ISO 15118’s Plug & Charge will allow authorization by means of certificates [10]. The authentication method used depends on the mobility service provider and often cannot be freely chosen by the CPO. So, only high-level security requirements are included for the terminal.

2.2.1.3 Electrical vehicle interface

The electric vehicle connects to the charging station on the electric vehicle interface, which is the power connection that will charge the car. In Europe, the main EV plug standards are IEC 62196 Type 2 [11] for AC chargers, and CCS Combo 2 [12] for DC chargers. The vehicle can communicate with the charging station to control charging. Now this is usually done through simple electrical signals. But in the future, there will be digital communication over the IEC 15118 protocol.

2.2.1.4 Local maintenance interface

Besides over the WAN through the CPO central system, engineers may also locally maintain the equipment through the local maintenance interface. This interface can be an Ethernet, serial, or USB port. Engineers connect an engineering laptop to the local maintenance interface and can configure the equipment using specialized management software or a web interface.

2.2.1.5 EMS interface

An energy management system (EMS) can be used for load balancing by connecting to the charging plazas or charging stations through the EMS interface. The EMS might set charging control limits to prevent overloading connections or due to weather conditions. The communication between the EMS and the charging station can be done through IEE 2030.5 protocol [13]. This interface is found only in certain charging stations, depending on the brand, model, and deployment (e.g., stand-alone or within a charging plaza).

2.2.2 Physical locations

Charging stations can be placed in public parking spaces, in parking garages, or at homes. A charge point operator can operate hundreds of thousands of charging stations spread over a large area. So, it is not realistic to physically protect them. Engineers only visit charging stations when there are problems or there is scheduled maintenance.

2.3 Access control policy

Table 1 lists the users that are authorized to access the EV charging station and the access they require. See Figure 2 for the interfaces. 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 charging station.

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 the charging	Authentication terminal
Electric vehicle	• Control the charging • *Optional:* authenticate for charging	Electric vehicle
Other charging stations	• Load balancing within a charging plaza	LAN
Local EMS	• Energy management within the local context (e.g., building)	LAN

3 Security objectives for charging stations

Below are the security objectives for a charging station that are the basis for the security requirements in Section 4.

7.4-CO1 Physical access detection on charging stations: The charging station sends an alert to the CSMS when any part of its casing is opened.

7.8-CO1 Tamper resistance on charging stations: The charging station has a casing that protects against physical manipulation, so that attackers without specialist tools cannot reach its internal components without leaving visible traces.

7.12-CO1 Cabling security for EMS connection: Network cables connecting a charging station to an EMS are protected against tampering. Attackers without specialist tools cannot physically connect to the EMS interface without leaving visible traces.

8.3-CO6 Least privileges on the WAN, authentication terminal, electric vehicle, LAN, and EMS interfaces: The charging station enforces access control on the WAN, authentication terminal, electric vehicle, LAN, and EMS interfaces, so that users on the interface can only access the functions they need.

8.5-CO4 Role-based authentication for the CSMS, electric vehicle, engineers, EMS, and other charging stations with unique authentication for the charging stations: The CSMS, electric vehicle, engineers, EMS, and other charging stations identify to the charging station with information that allows the charging station to determine its role. The charging station authenticates the system's role and assigns it access rights based on the role. The charging station uniquely identifies itself to CSMS, electric vehicle, engineers, EMS, and other charging stations and allows the system to authenticate them.

8.5-CO5 Authentication for EV drivers on the authentication terminal: The charging station enforces authentication for EV drivers on the authentication terminal using a mechanism chosen by the mobility service provider.

8.8-CO2 Hardened by default: The charging stations are delivered by the manufacturer in a hardened configuration. Unneeded functions are disabled to reduce

the likelihood of vulnerabilities. Security functions on the hardware and software platforms are enabled to reduce the possible impact of vulnerabilities.
8.9-CO2 Automated configuration management: The charging station can be restored from a backed-up configuration automatically by the CPO central system.
8.15-CO2 Collecting security events through the CPO central system: The charging station logs all relevant security events locally and sends selected events to the CPO central system, so that they can be analyzed to detect incidents. *Remark:* The CPO central system can forward the security logs to a SIEM system.
8.17-CO2 Clock synchronization: The charging station synchronizes time with a central source to have reliable timestamps for security events.
8.19-CO2 Automated firmware management for local controllers: The software and firmware on the local controller in the charging station can be updated through remote access from the CPO central system. The local controller checks the authenticity of firmware or software through digital signatures before installation.
8.20-CO2 Cryptographic protection of communication confidentiality and integrity on the WAN interface: The charging station protects the integrity and confidentiality of communication on the WAN interface using cryptographic measures. The measures allow to verify the source of messages and protect against replay and man-in-the-middle attacks.
8.20-CO3 Resilience of charging functions against denial-of-service attacks on the WAN: The charging station shields charging functions 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
8.22-CO2 Logical network segregation on the charging station WAN: The charging station is segregated from other zones on the WAN interface. Only normal connections are allowed through the network perimeter. The communication load can be controlled at the perimeter.
8.24-CO2 Automated key and password management over the WAN: All passwords and keys used in the charging station can be updated automatically through remote access from the CPO central system

3.1 Rationale for the component objectives

Each requirement is a direct translation of the system level objective in [4] with the same number. All technological objectives for the EV charging station are covered.

4 Security requirements

Section 3 sets security objectives for charging stations to align with the overall objectives for the EV charging infrastructure. These objectives refine the technological security controls in ISO/IEC 27002:2022 [9]. We now break down the objectives into more detailed requirements from IEC 62443-4-2 [1] that a system integrator or department building or maintaining an EV charging infrastructure can follow (Table 2). See Section 4.1 for the full list of requirements. The rationale for selecting the requirements is given in Section 4.2.

As mentioned in the introduction, it is recommended that besides the technological requirements selected here, grid operators also require that any software supplier complies full to **IEC 62443-4-1** [14] at **maturity level at least 2**. From 2024 onwards, it is recommended to require maturity level at least 3 for IEC 62443-4-1.

Table 2 Breakdown of objectives into IEC 62443-4-2 requirements

Security objective	***IEC 62443-4-2 requirements***
7.4 Physical security monitoring	
7.4-CO1 Physical access detection on charging stations: The charging station sends an alert to the CSMS when any part of its casing is opened.	• EDR 3.11 RE1 Notification of a tampering attempt
7.8 Equipment siting and protection	
7.8-CO1 Tamper resistance on charging stations: The charging station has a casing that protects against physical manipulation, so that attackers without specialist tools cannot reach its internal components without leaving visible traces.	• CR 7.7 Least functionality • EDR 2.13 Use of physical diagnostic and test interfaces • EDR 3.11 Physical tamper resistance and detection
7.12 Cabling security	
7.12-CO1 Cabling security for the EMS interface: Network cables connected on the EMS interface are protected against tampering. Attackers without specialist tools	• EDR 3.11 Physical tamper resistance and detection

cannot physically connect to the EMS interface without leaving visible traces.	
8.3 Information access restriction	
8.3-CO6 Least privileges on the WAN, authentication terminal, electric vehicle, LAN, and EMS interfaces: The charging station enforces access control on the WAN, authentication terminal, electric vehicle, LAN, and EMS interfaces, so that users on the interface can only access the functions they need.	• CR 2.1 Authorization enforcement • CR 2.1 RE1 Authorization enforcement for all users (humans, software processes and devices)
8.5 Secure authentication	
8.5-CO4 Role-based authentication for the CSMS, electric vehicle, engineers, EMS, and other charging stations: The CSMS, electric vehicle, engineers, EMS, and other charging stations identify to the charging station with information that allows the zone to determine its role. The zone authenticates the system's role and assigns it access rights based on the role. The charging station uniquely identifies itself to CSMS, EV driver, electric vehicle, and other charging stations, and allows the system to authenticate them.	• CR 1.1 Human user identification and authentication • CR 1.2 Software process and device identification and authentication • CR 1.9 Strength of public key-based authentication • CR 2.6 Remote session termination • CR 4.3 Use of cryptography
8.5-CO5 Authentication for EV drivers on the authentication terminal: The charging station enforces authentication for EV drivers on the authentication terminal using a mechanism chosen by the mobility service provider.	• CR 1.1 Human user identification and authentication
8.8 Management of technical vulnerabilities	
8.8-CO2 Hardened by default: The charging stations are delivered by the	• CR 7.7 Least functionality

manufacturer in a hardened configuration. Unneeded functions are disabled to reduce the likelihood of vulnerabilities. Security functions on the hardware and software platforms are enabled to reduce the possible impact of vulnerabilities.	• EDR 3.2 Protection from malicious code
8.9 Configuration management	
8.9-CO2 Automated configuration management: The charging station can be restored from a backed-up configuration automatically by the CPO central system.	• CR 7.3 Control system backup • CR 7.4 Control system recovery and reconstitution
8.15 Logging	
8.15-CO2 Collecting security events through the CPO central system: The charging station logs all relevant security events locally and sends selected events to the CPO central system, so that they can be analyzed to detect incidents. *Remark:* The CPO central system can forward the security logs to a SIEM system.	• CR 2.8 Auditable events • CR 2.9 Audit storage capacity • CR 2.10 Response to audit process failures • CR 3.9 Protection of audit information • CR 6.1 Audit log accessibility • CR 6.1 RE1 Programmatic access to audit logs
8.17 Clock synchronization	
8.17-CO2 Clock synchronization: The charging station synchronizes time with a central source to have reliable timestamps for security events.	• CR 2.11 Timestamps • CR 2.11 RE1 Time synchronization • CR 2.11 RE2 Protection of time source integrity
8.19 Installation of software on operational systems	
8.19-CO2 Automated firmware management for local controllers: The software and firmware on the local controller in the charging station or plaza can be updated through remote access from the CPO central system. The local controller	• CR 1.8 Public key infrastructure certificates • CR 1.9 Strength of public key-based authentication • CR 4.3 Use of cryptography • EDR 3.10 Support for updates

can check the authenticity of firmware through digital signatures before installation.	• EDR 3.10 RE1 Update authenticity and integrity • EDR 3.12 Provisioning supplier roots of trust
8.20 Network security	
8.20-CO2 Cryptographic protection of communication confidentiality and integrity on the WAN interface: The charging station protects the integrity and confidentiality of communication on the WAN interface using cryptographic measures. The measures allow to verify the source of messages and protect against replay and man-in-the-middle attacks.	• CR 1.9 Strength of public key-based authentication • CR 3.1 Communication integrity • CR 3.1 RE1 Communication authentication • CR 3.8 Session integrity • CR 4.1 Information confidentiality • CR 4.3 Use of cryptography
8.20-CO3 Resilience of charging functions against denial-of-service attacks on the WAN: The charging station shields charging functions 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	• CR 7.1 Denial-of-service protection
8.22 Segregation of networks	
8.22-CO2 Network segregation on the charging station WAN: The charging station is segregated from other zones on the WAN interface. Only normal connections are allowed through the network perimeter.	• CR 5.1 Network segmentation • NDR 5.2 Zone boundary protection • NDR 5.2 RE1 Deny all, permit by exception • CR 7.1 Denial of service protection • CR 7.1 RE1 Manage communication load
8.24 Use of cryptography	
8.24-CO2 Automated key and password management: All passwords and keys used in the charging station can be updated	• CR 1.5 Authenticator management

automatically through remote access from the CPO central system	• EDR 3.13 Provisioning asset owner roots of trust

4.1 Requirements selected from 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* [1]. We are using the embedded device requirement (EDR) from IEC 62443-4-2. We are assuming here that the RTU, or gateway is an embedded device, and is using the embedded device requirement (EDR) from IEC 62443-4-2.

We are assuming here that the charging station is an embedded device, so that the embedded device requirements (EDR) from IEC 62443-4-2 apply. One requirement for network devices (NDR 5.2) has been selected, as the charging station usually includes its own telecom modem.

Some of the requirements have been adapted to the specific application domain of EV charging infrastructure to be able to meet the security objectives. The adaptations are prescriptive. To be compliant with the requirements in this document all adaptations must be followed.

The adaptations should be read as a specification of the original requirement. The original requirement remains in force. The adaptation limits the options for meeting the requirements to ensure that the implementation meets the security objectives

Besides the adaptations, supplemental guidance is included for some requirements. The guidance is non-binding. It clarifies the requirements, gives examples, or provides recommendations on implementing the requirement.

Following the convention in IEC 62443-4-2 we use *'components'* for the charging station in the CR requirements, and *'embedded device'* in the EDR requirements.

IEC	Name	Obj
CR 1.1	**Human user identification and authentication** *Adaptation:* The charging station shall provide the capability to identify and authenticate the role of engineers. The charging station uniquely identifies itself to the human users and allows these to authenticate it.	8.5-CO4 8.5-CO5

IEC	Name	Obj
	The charging station shall identify and authenticate EV drivers on the authentication terminal using a mechanism chosen by the mobility service provider.	
CR 1.2	**Software process and device identification and authentication** *Adaptation:* The charging station shall provide the capability to identify and authenticate the role of 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. The charging station uniquely identifies itself to the software processes and devices and allows these to authenticate it. *Supplemental guidance:* Authentication is required on the electric vehicle interface only if data is exchanged on this interface, e.g., using the IEC 15118 protocol.	8.5-CO4
CR 1.5	**Authenticator management** *Adaptation:* Components shall be delivered with unique initial authenticators for the device during manufacturing. Components shall provide the capability to update all authenticators from the CPO central system over the WAN interface. It shall be possible to update them without support from the supplier. The confidentiality and integrity of the authenticators shall be protected during changes. Components shall at least protect passwords from unauthorized disclosure when stored by storing them salted and hashed. *Supplemental guidance:* The adaptation only concerns point c) and part of point d) of the original requirement. The rest of the requirement stays in force without adaptation.	8.24-CO2

IEC	Name	Obj
	Keys and credentials may be updated manually using the maintenance tools. When public-key cryptography is used, keys are preferably updated using an automated process, for instance using the use cases defined in the OCPP 2.0 standard. It is allowed that keys or credentials cannot be updated if they are only used for device internal purposes, such as encrypting local storage or setting up secure communication between processors on the same device. Allowing authenticators to be only updated through firmware updates does not meet the requirement, as preparing the firmware update would require support from the supplier. For storing passwords, it is recommended to use a hashing function that is resistant to GPU cracking attacks, such as Argon2 or PBKDF2.	
CR 1.8	**Public key infrastructure certificates**	8.19-CO2
CR 1.9	**Strength of public key-based authentication**	8.5-CO4 8.19-CO2 8.20-CO2
CR 2.1	**Authorization enforcement** *Adaptation:* The charging station shall provide the capability to implement the access control policy described in Table 1 in Section 2.3 implementing the principle of least privilege.	8.3-CO6
CR 2.1 RE1	**Authorization enforcement for all users (humans, software processes and devices)**	8.3-CO6
CR 2.6	**Remote session termination**	8.5-CO4

IEC	Name	Obj
CR 2.8	**Auditable events** *Supplemental guidance:* Access control events should include at least: • Successful authentications • Failed authentication attempts • Changing user accounts • Changing authorizations Configuration change events should include: • Firmware uploads • Successful firmware updates • Failed firmware updates • Changing the system time • Changing keys or credentials • Failed attempt to change keys or credentials The device should also generate events for shutting down and booting the device.	8.15-CO2
CR 2.9	**Audit storage capacity**	8.15-CO2
CR 2.10	**Response to audit process failures**	8.15-CO2
CR 2.11	**Timestamps**	8.17-CO2
CR 2.11 RE1	**Time synchronization**	8.17-CO2
CR 2.11 RE2	**Protection of time source integrity**	8.17-CO2
CR 3.1	**Communication integrity**	8.20-CO2
CR 3.1 RE1	**Communication authentication** *Adaptation:* Components shall provide the capability to verify the authenticity of information received on the WAN interface using cryptographic methods.	8.20-CO2

IEC	Name	Obj
	Supplemental guidance: The integrity and authenticity of the communication can be protected by using TLS, as defined in the OCPP 2.0 standard or the security extension to OCPP 1.6.	
CR 3.8	**Session integrity**	8.20-CO2
CR 3.9	**Protection of audit information** *Supplemental guidance:* Audit information and audit logs must be persistent under reboots of the component and firmware updates. According to the access control policy access control policy in Table 1 in Section 2.3, it must be possible to restrict access to the audit information and audit logs to infrastructure administrators. See also CR 2.1.	8.15-CO2
CR 4.1	**Information confidentiality** *Adaptation:* Components shall support the protection of the confidentiality of information in transit on the WAN interface using encryption. Information at rest may be protected by access control mechanisms and physical protection. Cryptographic protection is not required at rest. *Supplemental guidance:* Confidentiality of the communication can be protected by using TLS, as defined in the OCPP 2.0 standard or the security extension to OCPP 1.6.	8.20-CO2
CR 4.3	**Use of cryptography** *Supplemental guidance:* Guidance on cryptographic algorithms and key lengths is given in: • the ANSSI selection guide for cryptographic algorithms [15] and rules and recommendations on the choice and parameters of cryptographic algorithms [16]	8.5-CO4 8.19-CO2 8.20-CO2

IEC	Name	Obj
	• the BSI technical guideline *Cryptographic Mechanisms: Recommendations and Key Lengths* [17] • the ECRYPT – *Algorithms, Key Size, and Protocols Report* [18] • the NIST *Recommendation for key management* [19] The latest version of these reports should be followed. Algorithms and key sizes should be used that are recommended for new systems at the time of deployment, and preferably also for the full lifetime of the product. A dedicated cryptographic (pseudo-)random number generator should be used to generate random numbers for all security functions.	
CR 5.1	**Network segregation**	8.22-CO2
CR 6.1	**Audit log accessibility**	8.15-CO2
CR 6.1 RE1	**Programmatic access to audit logs** *Adaptation:* Components shall allow the CSMS to collect security events. *Supplemental guidance:* 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.	8.15-CO2
CR 7.1	**Denial-of-service protection** *Supplemental guidance:* The essential functions in this case are at least the charging transactions. Customers should be able to continue charging even	8.20-CO3 8.22-CO2

IEC	Name	Obj
	when there is a denial-of-service attack on the WAN interface.	
CR 7.1 RE1	**Manage communication loads**	8.22-CO2
CR 7.3	**Control system backup**	8.9-CO2
CR 7.4	**Control system recovery and reconstitution**	8.9-CO2
CR 7.7	**Least functionality** *Adaptation:* The charging station 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 • all debug, diagnostic, or test interfaces disabled Hardware, debug, diagnostic, and test interface shall be disabled through one-time programmable memory (OTP) or muxing.	8.8-CO2 7.8-CO1
EDR 2.13	**Use of physical diagnostic and test interfaces**	7.8-CO1
EDR 3.2	**Protection from malicious code** *Adaptation:* The device shall be delivered with the security features from the underlying hardware and operating system enabled whenever possible. *Supplemental guidance:* 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.	8.8-CO2

IEC	Name	Obj
	- 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.	
EDR 3.10	**Support for updates** *Adaptation:* The charging station shall allow updates to be performed over the WAN interface by a centralized system and over the local maintenance interface by engineers. The charging station shall have enough memory (RAM and flash) and computing power to allow security updates needed during its lifetime. *Supplemental guidance:* Updates should be performed through a controlled process. See for instance, IEC 62443-2-4 requirement SP.11 [20]. The component should not automatically apply security updates without permission of the engineer. 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 the ECRYPT report [18] 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.	8.19-CO2
EDR 3.10 RE1	**Update authenticity and integrity** *Adaptation:* Components shall validate the authenticity and integrity of any software or firmware	8.19-CO2

IEC	Name	Obj
	update by validating a digital signature before installing it. The update shall be signed by the supplier. The signature shall protect the entire update. *Supplemental guidance:* It is not required that the integrity or authenticity of the firmware or software is validated during boot ("secure boot"). The embedded device should not allow the mechanisms that protect the authenticity and integrity of software updates to be bypassed through the recovery process, required by CR 7.4.	
EDR 3.11	**Physical tamper resistance and detection** *Adaptation:* The charging station shall provide tamper resistance and detection mechanisms to protect the cabling on the EMS interface. The mechanisms shall ensure that attackers without specialist tools cannot physically connect to the EMS interface without leaving visible traces.	7.8-CO1 7.12-CO1
EDR 3.11 RE1	**Notification of a tampering attempt** *Supplemental guidance:* Alerts for opening the casing are included in the OCPP 2.0 standard and the security extension to OCPP 1.6.	7.4-CO1
EDR 3.12	**Provisioning product supplier roots of trust**	8.19-CO2
EDR 3.13	**Provisioning asset owner roots of trust**	8.24-CO1
NDR 5.2	**Zone boundary protection**	8.22-CO2
NDR 5.2 RE1	**Deny all, permit by exception**	8.22-CO2

4.2 Rationale for the requirements

Below a rationale is provided for the requirements selected in Sections 4.1 by showing that they cover the security objectives for the device.

7.4-CO1 Physical access detection on charging stations

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

7.8-CO1 Tamper resistance on charging stations

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.

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*).

7.12-CO1 Cabling security for EMS connection

Security for the cabling on the EMS interface ensures that a physical connection to the EMS interface is not possible for attackers with moderate resources (*EDR 3.11*)

8.3-CO6 Least privileges on the WAN, authentication terminal, electric vehicle, LAN, and EMS interfaces

Authorization for all users is covered by *CR 2.1* and *CR 2.1 RE1.* No requirements on account management are included, as there may not be a clear account associated with the access if, for instance, a VPN is used.

8.5-CO4 Role-based authentication for the CSMS, electric vehicle, engineers, EMS, and other charging stations

The objective concerns both human users and software process users.

Authentication for human users is covered by requirement *CR 1.1* with the adaptation to allow the identification of roles.

Authentication for software process users is covered by requirement *CR 1.2* with the adaptation to ensure mutual authentication.

Strong cryptographic keys and algorithms for the authentication are ensured by requirements *CR 1.9* and *CR 4.3*. Remote session termination (*CR 2.6*) is included to reduce the risk that authentication is bypassed by compromising a session.

8.5-CO5 Authentication for EV drivers on the authentication terminal

Authentication for human users is covered by requirement *CR 1.1*. The adaptation ensures that the charging station supports the authentication mechanism specified by the mobility service provider.

8.8-CO2 Hardened by default

Disabling unneeded functions is covered by requirement *CR 7.7*, enabling security features of the platform by *EDR 3.2*. The requirement is adapted to clarify the measures against malicious code that are at least required. The adaptation to *CR 7.7* ensures that the device is delivered in a secure state.

8.9-CO2 Automated configuration management

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

8.15-CO2 Collecting security events through the CPO central system

Requirement *CR 2.8* ensures that security events are logged, while requirements *CR 6.1* and *CR 6.1 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 *CR 2.10* and *CR 3.9*. Requirement *CR 2.9* ensures that there is enough storage capacity on the device for the logs.

8.17-CO2 Clock synchronization

Clock synchronization is covered by requirements *CR 2.11* and *CR 2.11 RE1*. Requirement *CR 2.11 RE2* ensures that the integrity of the time source is protected.

8.19-CO2 Automated firmware management

Updates of software and firmware are covered by *EDR 3.10*. The adaptation ensures that the updates can be performed remotely and that 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*, and the adaptation ensures that the digital signature cannot be bypassed through the recovery process. Requirement *CR 1.8* and EDR 3.12 ensure that the device can be integrated into the supplier’s PKI for the certificates needed to verify the signature. Requirements *CR 1.9* and *CR 4.3* ensure the strength of the cryptography used for the signatures.

8.20-CO2 Cryptographic protection of communication confidentiality and integrity on the WAN and remote maintenance interfaces

Protecting the confidentiality of the information is covered by requirement *CR 4.1*. Integrity of the communication by *CR 3.1*, *CR 3.1 RE1*, and *CR 3.8*. Requirements *CR 1.9* and *CR 4.3*, ensure that strong cryptography is used to protect the communication.

8.20-CO3 Resilience of charging functions against denial-of-service attacks on the WAN

Resilience against denial-of-service attacks is provided by requirement *CR 7.1*.

8.22-CO2 Logical network segregation on the charging station WAN

Network segregation is ensured by requirement *CR 5.1*.

Requirements *NDR 5.2* and *NDR 5.2 RE1* ensure that there is protection between different security zones, and only allowed traffic can go through.

Protection against denial-of-service attacks on the WAN is achieved by requirements *CR 7.1* and *CR 7.1 RE1*.

8.24-CO2 Automated key and password management

Automated updates of keys and credentials are covered by requirement *CR 1.5.* The adaptation 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 into their PKI.

Appendix A: 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 [21] or OCPP 1.6 [22] with the security whitepaper [23] used by many charging stations.

A.1 Requirements fully covered by OCPP 2.0

The requirements in Table 3 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 including possible adaptations.

Table 3: Requirements fully covered by OCPP 2.0.

Requirement	**Section in [21]**	**OCPP Implementation**
CR 2.8 Auditable events	Appendix 1. Security events	The required events are logged if all events in Appendix 1 are logged.
EDR 3.10 Support for updates	L. Firmware management	OCPP 2.0 defines use cases for remotely updating the firmware.
EDR 3.10 RE1 Update authenticity and integrity EDR 3.12 Provisioning supplier roots of trust	L.2.L01	The secure firmware update process defined in OCPP 2.0 use case L01 uses digital signatures. Note that to meet the requirement, non-secure firmware updates (use case L02) should be disabled.
EDR 3.11 Physical tamper resistance and detection	Appendix 3.2.10 CaseAccessSensor	Appendix 3.2.10 describes the tamper detection sensor that reports when a door/panel is open.
EDR 3.11 RE1 Notification of a tampering attempt	Appendix 1	TamperDetectionActivated is marked as a critical event.

A.2 Requirements partially covered by OCPP 2.0

The requirements in Table 4 (including possible adaptations) 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 4: Requirements partially covered by OCPP 2.0.

Requirement	Section in [21]	OCPP Implementation
CR 1.2 EE1 Role-based identification and authentication for software processes and devices with unique authentication for the charging stations	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.
CR 1.5 Authenticator management CR 1.5 EE2: Remote authenticator update EDR 3.13 Provisioning asset owner roots of trust	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.
CR 1.9 Strength of public key-based authentication	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.
CR 2.1 Authorization enforcement CR 2.1 RE1 Authorization enforcement for all users (humans, software processes and devices)	-	The OCPP protocol implicitly defines the access rights of the CSMS by describing which functions are exposed over OCPP.

CR 3.1 Communication integrity CR 3.1 RE1 Communication authentication CR 3.8 Session integrity	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.
CR 4.1 Information confidentiality	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.
CR 4.3 Use of cryptography CR 4.3 EE1 Use of cryptography according to ECRYPT recommendations	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.
CR 6.1 Audit log accessibility CR 6.1 EE1 Restricted access to audit logs CR 6.1 RE1 Programmatic access to audit logs	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.

Glossary

AC	Alternating Current
APN	Access Point Name
CPO	Charge Point Operator
CSMS	Charging Station Management System
CVSS	Common Vulnerability Scoring System
DC	Direct Current
DSO	Distribution System Operator
EMS	Energy Management System
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
GDPR	General Data Protection Regulation
GPRS	General Packet Radio Service
IACS	Industrial Automation and Control System
LAN	Local Area Network

References

[1] 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.

[2] M. A. Sayed, M. Ghafouri, M. Debbabi and C. Assi, "Dynamic Load Altering EV Attacks Against Power Grid Frequency Control," *IEEE Power & Energy Society General Meeting (PESGM),* pp. 1-5, 2022.

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

[4] ENCS, EV-111-2022 Threat analysis for EV charging infrastructure, 2022.

[5] IEC, "IEC 62443-1-5: Rules for IEC 62443 profiles," 2022.

[6] Joint Research Center, "Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme," 2020.

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

[8] ENCS, EV-211-2022: IEC 62443 security requirements for EV charging infrastructure, 2022.

[9] ISO/IEC , "ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls," 2022.

[10] Elaad NL, Public Key Infrastructure for ISO 15118 - Freedom of choice for consumers & an open access market, 2022.

[11] IEC, IEC 62196-2:2022 Plugs, socket-outlets, vehicle connectors and vehicle inlets - Conductive charging of electric vehicles - Part 2: Dimensional compatibility requirements for AC pin and contact-tube accessories, 2022.

[12] IEC, IEC 62196-3:2022 Plugs, socket-outlets, vehicle connectors and vehicle inlets - Conductive charging of electric vehicles - Part 3: Dimensional compatibility requirements for DC and AC/DC pin and contact-tube vehicle couplers.

[13] Elaad NL, EV Related Protocol Study, 2016.

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

[15] ANSSI, "ANSSI-PA-079: Guide de Sélection d'algorithmes cryptographiques," 2021.

[16] ANSSI, "ANSSI-PG-083: Guide de mécanismes cryptographiques: Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques," 2020.

[17] Federal Office for Information Security, "BSI - Technical Guideline TR-02101-1: Cryptographic Mechanisms: Recommendations and Key Lengths," 2022.

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

[19] National Institute for Standards and Technology, "NIST Special Publication 800-57 Part 1 Revision 5: Recommendation for Key Management: Part 1 - General," 2020.

[20] IEC, "IEC62443-2-4: Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers," 2015.

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

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

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

ENCS