



EV-311

Security requirements from IEC 62443 for procuring EV charging stations

Version 2026v2.0

13 October 2026

This document was produced by ElaadNL and ENCS as part of a 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/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	EV-301-2016 v1.0	EV Charging Systems Security Requirements
December 2019	EV-301-2019 v2.0	Security requirements for procuring EV charging stations
February 2025	2025v1.0	EV charging station security requirements. Aligned with threat analysis EV-111 2025v1.0.
September 2025	2025v1.1	Minor fixes
August 2026	2026v2.0	This revised version includes additional remote maintenance options resulting from the collaboration with the BEÖ NIS2 Working Group, whose members include the major Austrian CPOs 

Table of Contents

Version History	3
1 Introduction	5
1.1 Relation to other documents	6
2 Device description	7
2.1 Intended use of the device	7
2.1.1 Charging station management	8
2.1.2 Charging station maintenance	8
2.2 Intended operational environment	9
2.2.1 Interfaces	9
2.2.2 Physical locations	11
2.3 Users and access rights	11
3 Security requirements	12
4 Rationale for the requirements	23
Annex 1 – Requirements for a direct supplier connection	28
A1.1 Users and access rights	28
A1.2 Additional requirements to the charging station	28
A1.2.1 Additional objectives	29
A1.2.2 Security requirements	30
A1.3 Requirements to the supplier maintenance system	32
Glossary	34
References	35

1 Introduction

This document gives security requirements that Charge Point Operators (CPOs) 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 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 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 have since 2016 published a set of harmonized security requirements that CPOs can use to procure charging stations. The new version of the requirements in this document is based on the IEC 62443 standard. They have been selected from part *IEC 62443-4-2: Technical security requirements for IACS components* [1]. 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 [3] they form a profile for IEC 62443 (following the rules in [4]).

The ENCS and ElaadNL requirements are frequently used in tenders by local governments purchasing public charging stations. So, by applying the requirements CPOs can prepare for such tenders.

CPOs can also use the requirements to show to regulators that they are taking steps to mitigate cybersecurity risks. CPOs now fall under the EU NIS 2 directive and the network code for cybersecurity. According to these regulations, they must take measures to manage their cybersecurity risks.

From 1 August 2025, charging stations in the EU that use wireless communication will also need to comply with the cybersecurity requirements in the Radio Equipment Directive, following a delegated regulation from the European Commission in 2022 [5]. Manufacturers can meet these requirements by implementing the harmonized standard EN 18031. The requirements in this document have been aligned with EN 18031 to make it easier for manufacturers to comply with both.

1.1 Relation to other documents

This document is part of a larger series on EV charging infrastructure security:

- *EV-111 Security threat analysis for EV charging infrastructure* [3] 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 [6].
- *EV-211: Security requirements from IEC 62443 for EV charging infrastructure* [6] gives security requirements for the EV charging infrastructure as a system, selected from the IEC 62443-3-3 standard. The requirements can be used to procure EV charging services from a CPO.
- *EV-312: Implementing IEC 62443-4-2 requirements in OCPP 2.0.1* [7] provides guidance on how the requirements in this document can be implemented in the OCPP 2.0.1 protocol.
- *EV-313: Coverage of EN 18031 requirements by the IEC 62443 requirements for EV charging stations* [8] shows how the requirements in the harmonized standard EN 18031 for the Radio Equipment Directive are covered by the requirements in this document.

2 Device description

The security requirements make certain assumptions on the intended use of the charging station, its intended operational environment, and the access control used for it. This section describes these assumptions.

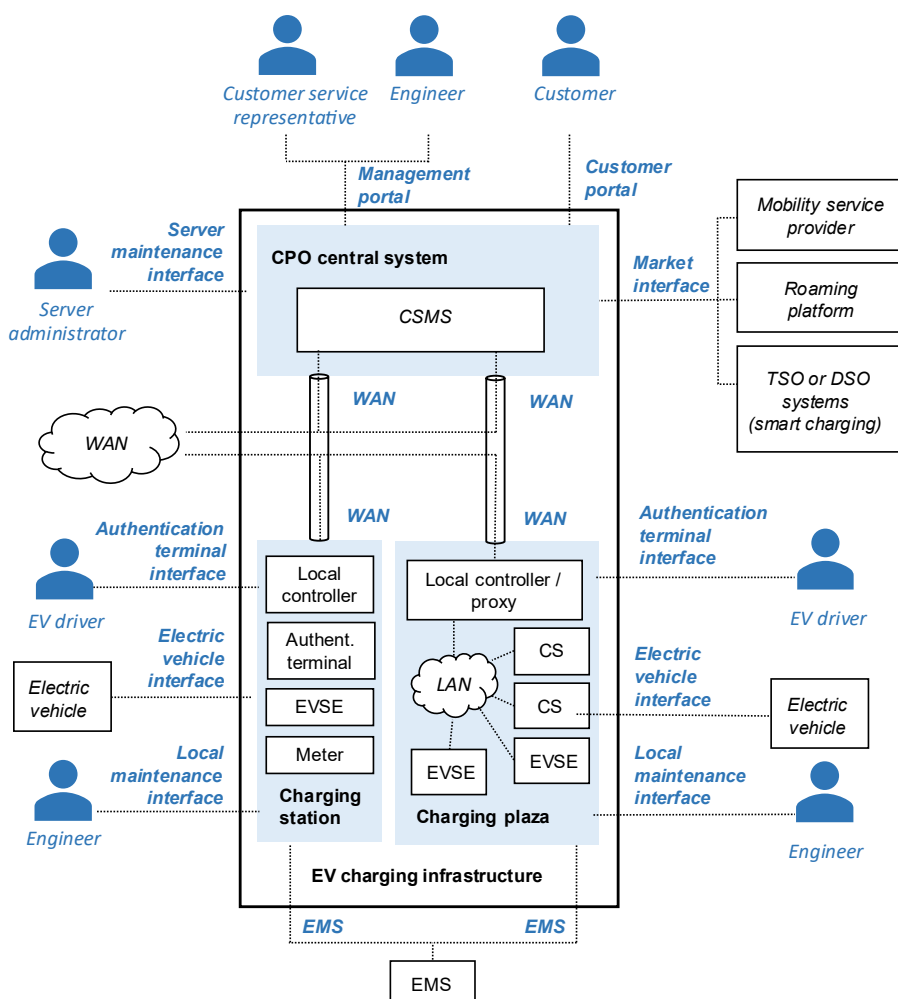


Figure 1: Reference architecture for the EV charging infrastructure, showing its users and interfaces. The requirements in this document concern the EV charging station.

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 some privately owned charging stations.

2.1.1 Charging station management

The CPO controls the charging stations through a charging station management system (CSMS). The charging station sends information on transactions to the CSMS for billing. The CSMS can send information on tariffs to the charging station. The CSMS is also used to configure and maintain the charging stations. If the charging stations are used for smart charging, the CSMS can adjust the charging speed to help CPOs solve load balancing or congestion problems in the electricity grid.

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 the communication between the local controller or between the different charging stations in the charging plaza are not considered here.

2.1.2 Charging station maintenance

The maintenance of the charging station can be done locally or remotely. This document includes two methods for remote access to the charging station or plaza by engineers from the charging station supplier (see Figure 2):

- **Connection through the CPO's central system only (default method).** The charging station connects to the CPO's CSMS through the WAN. All configuration and maintenance activities are performed through the CSMS. The charging station supplier's maintenance engineers access the charging station through the CPO's management system. The charging station does not connect directly to the supplier's systems.
- **Direct supplier connection enabled by the CPO (alternative method).** The charging station can connect directly to the supplier's systems through a separate connection through the WAN. This connection must first be enabled by the CPO through the CSMS and is disabled by default.

This document presents the connection through the CPO's central system as the default method throughout the document. The additional security objectives and security requirements needed for the alternative method, where a direct connection to the supplier is enabled by the CPO, are defined in **Annex 1**

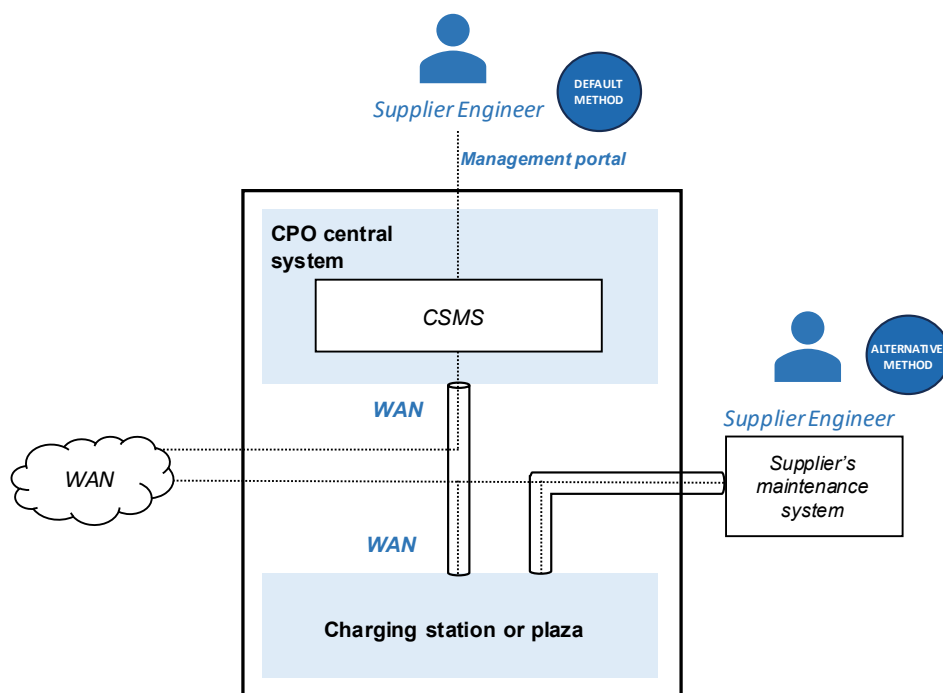


Figure 2 Methods for remote access to the EV charging station for maintenance

2.2 Intended operational environment

The intended operational environment of the EV charging infrastructure is shown in the reference architecture (Figure 1).

2.2.1 Interfaces

The EV charging station is connected to the operational environment on the interfaces listed in Table 1.

Table 1 Interfaces connecting the charging station to the operational environment.

Interface	Description
WAN	The charging station is connected to the CPO central system over a wide-area network (WAN). 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).

	The WAN interface may also be used for remote maintenance, either through the CPO's CSMS using OCPP or through a separate CPO-controlled connection, such as a second SIM.
Authentication terminal	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 [9]. 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.
Electric vehicle	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 [10] for AC chargers, and CCS Combo 2 [11] for DC chargers. The vehicle can communicate with the charging station to control charging. For DC charging, digital communication over protocols such as DIN SPEC 70121 [12] or ISO 15118 is used. In the future, AC charging will also use digital communication
Local maintenance	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.
EMS	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 Users and access rights

Table 2 lists the users that are authorized to access the EV charging station, the access they require, and the interfaces they use.

Table 2 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 <i>Optional:</i> Pay for the charging	Authentication terminal
Electric vehicle	- Control the charging <i>Optional:</i> authenticate for charging	Electric vehicle
Local EMS	Energy management within the local context (e.g., building)	LAN

3 Security requirements

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. One requirement for network devices (NDR 5.2) has been selected, as the charging station usually includes its own telecom modem.

When CPOs use the technical requirements below, it is recommended to also require that the supplier complies fully with **IEC 62443-4-1 [14] at maturity level at least 2**. Doing so ensures that the supplier has secure development processes, so that they can correctly and consistently implement the requirements. From 2027 onwards, it is recommended to require maturity level at least 3 for IEC 62443-4-1.

Some of the requirements have been contextualized to the specific application domain of EV charging infrastructure to be able to meet the security objectives. The **contextualizations** are prescriptive. To be compliant with the requirements in this document all contextualizations must be followed. The contextualizations should be read as a specification of the original requirement. The original requirement remains in force. The contextualization limits the options for meeting the requirements to ensure that the implementation meets the security objectives in Section 4.

Besides the contextualizations, **implementation 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.

Table 3 Full list of requirements selected from IEC 62443-4-2 for charging stations.

IEC	Name
CR 1.1	Human user identification and authentication <i>Contextualization - authentication for engineers:</i> The component shall provide the capability to identify the role of engineers, and to authenticate the role information. <i>Contextualization - authentication for EV drivers:</i> The component shall identify and authenticate EV drivers on the authentication terminal using a mechanism chosen by the mobility service provider.

IEC	Name
	<i>Implementation guidance:</i> Engineers may use shared passwords on the local maintenance interface, although it is recommended to use unique passwords per charging station or centrally managed accounts with individual passwords for the engineers.
CR 1.2	Software process and device identification and authentication
CR 1.2 RE1	Unique identification and authentication <i>Contextualization – unique authentication for the CSMS:</i> The component shall provide the capability to uniquely identify and authenticate itself to the CSMS, and to enforce that the CSMS and electric vehicle uniquely identifies and authenticates itself to the component before giving it access. <i>Contextualization – unique authentication for the electric vehicles:</i> If the component is exchanging data with electric vehicles (for instance using the IEC 15118 protocol), the component shall provide the capability to uniquely identify and authenticate itself to the electric vehicles, and to enforce that the electric vehicles uniquely identify and authenticates itself to the component before giving it access. <i>Implementation guidance:</i> Authentication is not required for an EMS connecting to the charging station. Instead, the connection to the EMS is protected by tamper detection (see requirement EDR 3.11). It would however be recommended to use mutual authentication also for the EMS. For OCPP communication, the authentication can be provided by the TLS with Basic Authentication or TLS with Client-Side Certificates profile. The IEC 15118 protocol also includes authentication using certificates.
CR 1.5	Authenticator management
	<i>Contextualization – authenticator updates from the CSMS:</i> Components shall provide the capability for the CPO central system to update all authenticators used on 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. <i>Contextualization - password storage:</i> components shall provide the capability to protect passwords from unauthorized disclosure by at least storing them salted and hashed.

IEC	Name
	<i>Contextualization – factory default passwords:</i> If a factory default password is used for an authentication mechanism required by CR 1.1 or CR 1.2, the password shall either be unique for each charging station or be enforced to be changed by the user before or on first use. <i>Implementation guidance:</i> The contextualizations only concern point c) and part of point d) of the original requirement. The rest of the requirement stays in force without contextualization. When public-key cryptography is used, keys are preferably updated using an automated process, for instance using the use cases defined in the OCPP 2.0.1 standard. Allowing authenticators used for remote access to be only updated through firmware updates does not meet the requirement, as preparing the firmware update would require support from the supplier. Keys and credentials used for local access may be updated manually using the maintenance tools. It is, however, recommended that they can be also remotely updated. 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. For storing passwords, it is recommended to use a hashing function that is resistant to GPU cracking attacks, such as Argon2 or PBKDF2.
CR 1.7	Strength of password-based authentication
CR 1.8	Public key infrastructure certificates
CR 1.9	Strength of public key-based authentication
CR 2.1	Authorization enforcement
CR 2.1 RE1	Authorization enforcement for all users (humans, software processes and devices)

IEC	Name
	<i>Contextualization – separation of roles:</i> The component shall provide the capability to separate the following roles to implement the principle of least privilege: • CSMS • Engineer • EV driver • Electric vehicles • EMS <i>Implementation guideline:</i> For more information, refer to the users and access rights in Table 2 in Section 2.3. Roles can be separated in different ways. The EV driver and electric vehicle role are usually separated by having them access their own interface. Roles could also be separated by using separate network services on the same interface. If roles use the same network service, they can be separated by role-based access rights.
CR 2.6	Remote session termination
CR 2.8	Auditable events <i>Implementation guidance:</i> 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.

IEC	Name
	If the OCPP protocol is used, these events are all covered by the security events in Appendix 1 of OCPP 2.0.1 or the security extension to OCPP 1.6.
CR 2.9	Audit storage capacity <i>Contextualization – sufficient resources:</i> The charging station shall have enough memory (RAM and flash) and computing power to allow recorded events to be saved for at least 30.
CR 2.10	Response to audit process failures <i>Implementation guidance:</i> If charging stations use OCPP, they can respond to the audit storage capacity being reached using a MemoryExhaustion alert. If the security log is full, it would be recommended to overwrite the oldest log entries.
CR 2.11	Timestamps
CR 2.11 RE1	Time synchronization <i>Implementation guidance:</i> OCPP includes different time sources: OCPP Heartbeat messages, NTP, GPS, real time clocks, mobile networks, and low frequency radio time transmitters.
CR 2.11 RE2	Protection of time source integrity <i>Implementation guidance:</i> If the charging station uses OCPP Heartbeat messages for time synchronization, the integrity of the messages can be protected using TLS (see requirement CR 3.1 RE1 below). Other protocols, such as NTP and GPS, do not have standard integrity protection built into the protocol. CPOs should assess the possible security risks when using such protocols.
CR 3.1	Communication integrity
CR 3.1 RE1	Communication authentication

IEC	Name
	<i>Contextualization – authentication of WAN communication:</i> Components shall provide the capability to verify the authenticity of information received on the WAN interface using cryptographic methods. <i>Implementation guidance:</i> The integrity and authenticity of the communication can be protected by using TLS, as defined in the OCPP 2.0.1 standard or the security extension to OCPP 1.6.
EDR 3.2	Protection from malicious code <i>Contextualization – hardware security features:</i> The device shall be delivered with the security features from the underlying hardware and operating system enabled whenever possible. <i>Implementation guidance:</i> It is recommended to use the following hardware features when they are supported: • No-Execute (NX) / Write-XOR-Execute (W^XR): 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.
CR 3.5	Input validation <i>Contextualization – no known vulnerabilities:</i> The device shall not contain publicly known exploitable vulnerabilities unless: • the vulnerability cannot be exploited in the specific conditions of the equipment, or • the vulnerability has been mitigated <i>Contextualization – testing for input validation vulnerabilities:</i> The supplier shall test each firmware version for input validation vulnerabilities using all activities described in requirement SVV-3 in IEC 62443-4-1 and fix or mitigate all vulnerabilities found before releasing the firmware.

IEC	Name
	<i>Implementation guidance:</i> The supplier should pay special attention to complex input files. This requirement also applies to charging cable communication when the electric vehicle interface supports DIN SPEC 70121 or ISO 15118.
CR 3.8	Session integrity
CR 3.9	Protection of audit information
	<i>Implementation guidance:</i> Audit information and audit logs must be persistent under reboots of the component and firmware updates. According to the access control policy in Table 2 in Section 2.3, it must be possible to restrict access to the audit information and audit logs to the CSMS and engineers. See also CR 2.1.
EDR 3.10	Support for updates
	<i>Contextualization – remote updates:</i> The charging station shall allow software and firmware updates to be performed over the WAN interface by the CPO central system and over the local maintenance interface by engineers. <i>Contextualization – sufficient resources:</i> The charging station shall have enough memory (RAM and flash) and computing power to allow security updates needed during its lifetime. <i>Implementation guidance:</i> Updates should be performed through a controlled process. See for instance, IEC 62443-2-4 requirement SP.11 [15]. 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 [16] 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.

IEC	Name
EDR 3.10 RE1	Update authenticity and integrity <i>Contextualization – signed firmware and software updates:</i> Components shall validate the authenticity and integrity of any software or firmware update by validating a digital signature before installing it. The update shall be signed by the supplier. The signature shall protect the entire update. <i>Implementation guidance:</i> 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 <i>Contextualization – protection against physical manipulation:</i> The charging station casing shall protect against physical manipulation, so that attackers without specialist tools cannot reach its internal components without leaving visible traces. <i>Contextualization – protection against tampering on the EMS interface:</i> 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.
EDR 3.11 RE1	Notification of a tampering attempt <i>Implementation guidance:</i> Alerts for opening the casing are included in the OCPP 2.0.1 standard and the security extension to OCPP 1.6.
EDR 3.12	Provisioning product supplier roots of trust
EDR 3.13	Provisioning asset owner roots of trust
CR 4.1	Information confidentiality

IEC	Name
	<i>Contextualization – encryption of WAN communication:</i> Components shall support the protection of the confidentiality of information in transit of all communication on the WAN interface using encryption. <i>Contextualization - protection of information at rest:</i> Information at rest may be protected by access control mechanisms and physical protection. Cryptographic protection is not required at rest. <i>Implementation guidance:</i> Confidentiality of the communication can be protected by using TLS, as defined in the OCPP 2.0.1 standard or the security extension to OCPP 1.6.
CR 4.2	Information persistence <i>Contextualization – deletion of personal information:</i> Components shall be able to delete any personal information stored on it on request of the CSMS. <i>Implementation guidance:</i> Transaction information and information used for charging authorizations could include information used to identify individual EV users, such as the UUID of their charging card. Such information should be considered personal information.
CR 4.3	Use of cryptography <i>Implementation guidance:</i> Guidance on cryptographic algorithms and key lengths is given in: - the ANSSI selection guide for cryptographic algorithms [17] and rules and recommendations on the choice and parameters of cryptographic algorithms [18] - the BSI technical guideline <i>Cryptographic Mechanisms: Recommendations and Key Lengths</i> [19] - the ECRYPT – <i>Algorithms, Key Size, and Protocols Report</i> [16] - the NIST <i>Recommendation for key management</i> [20] 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.

IEC	Name
	A dedicated cryptographic (pseudo-)random number generator should be used to generate random numbers for all security functions. The OCPP specification defines the cryptographic protocols that are allowed for its implementation. These protocols are in line with the guidance referenced above.
NDR 5.2	Zone boundary protection <i>Contextualization – firewalling on WAN interface:</i> If the charging station has an integrated telecom modem for communication on the WAN interface, the modem shall act as a firewall to monitor and control communication on the WAN interface.
NDR 5.2 RE1	Deny all, permit by exception <i>Contextualization – Connection only to the CSMS:</i> the component shall allow only connections to the CSMS. Direct connections to the charging station suppliers shall not be permitted. <i>Implementation guidance:</i> The charging station shall only have a SIM card that communicates with the CSMS. A second SIM card to communicate with the charging station supplier is not allowed. To support the alternative remote maintenance connection through a SIM card, see the security requirements in Annex 1.
CR 6.1	Audit log accessibility
CR 6.1 RE1	Programmatic access to audit logs <i>Contextualization – audit logs collected by CSMS:</i> Components shall allow the CSMS to collect security events. <i>Implementation guidance:</i> In OCPP 2.0.1 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.
CR 7.1	Denial-of-service protection <i>Implementation guidance:</i> The essential functions in this case are at least the charging transactions. Customers should be able to continue charging even when there is a denial-of-service attack on the WAN interface.

IEC	Name
CR 7.4	Control system recovery and reconstitution <i>Contextualization – restoration from CPO central system:</i> Components shall have the capability to be restored from a backed-up configuration by the CPO central system.
CR 7.6	Network and configuration settings <i>Contextualization – secure configuration by default:</i> The component shall be delivered by the manufacturer with the recommended network and security configurations.
CR 7.7	Least functionality <i>Contextualization – hardened by default:</i> Components 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 external hardware ports disabled <i>Implementation guidance:</i> Hardware, debug, diagnostic, and test interface should be disabled through one-time programmable memory (OTP) or muxing. Unused network services should be disabled from all interfaces, including all unused network services in the electric vehicle interface when supporting DIN SPEC 70121 or ISO 15118.

4 Rationale for the requirements

The requirements in Section 4 have been chosen based on the security objectives derived in the threat analysis for EV charging infrastructure [3]. The system-level objectives from the objectives have first been translated into component-level objectives for the charging station. The security requirements for IEC 62443-4-2 [1] have been selected to cover the objectives.

Table 4 shows the component-level security objectives and the corresponding security requirements from IEC 62443-4-2. Each component-level objective is a direct translation of the system level objective in [3] with the same number. The objectives are linked to controls from the ISO/IEC 27002:2022 standard [21], as many CPOs are using an ISO/IEC 27000 based information security management system. All physical and technological system-level objectives for the EV charging station are covered. The organizational and physical objectives should be met separately by the CPO as explained in the security requirements for EV charging infrastructure [6].

Table 4 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 Physical tamper resistance and detection • 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.	• EDR 3.11 Physical tamper resistance and detection • CR 7.7 Least functionality
7.12 Cabling security	
7.12-CO1 Cabling security for the EMS interface: Network cables connected on the EMS interface are protected against	• EDR 3.11 Physical tamper resistance and detection

tampering. Attackers without specialist tools 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, local maintenance, LAN, and EMS interfaces: The charging station enforces access control on the WAN, authentication terminal, electric vehicle, local maintenance, 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 engineers: The engineers identify to the charging station with information that allows the zone to determine its role. The charging station authenticates the role information and assigns the engineer access rights based on the role.	• CR 1.1 Human user identification and authentication • CR 2.1 RE1 Authorization enforcement for all users (humans, software processes and devices)
8.5-CO5 Unique authentication for the CSMS and electric vehicles: The CSMS and electric vehicles uniquely identify themselves to the charging station. The charging station authenticates their identity and assigns them access rights based on their role.	• CR 1.2 Software process and device identification and authentication • CR 1.2 RE1 Unique 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-CO6 Authentication for EV drivers on the authentication terminal: The charging station enforces authentication for EV drivers on the authentication terminal using	• CR 1.1 Human user identification and authentication • CR 2.1 RE1 Authorization enforcement for all users (humans, software processes and devices)

a mechanism chosen by the mobility service provider.	
8.8 Management of technical vulnerabilities	
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. The device does not contain publicly known vulnerabilities that can be exploited on the device.	• CR 3.5 Input validation • EDR 3.2 Protection from malicious code • CR 7.7 Least functionality
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 7.4 Control system recovery and reconstitution
8.9-CO3 Secure configuration by default: The charging station is delivered by the manufacturer with a secure configuration. Unneeded functions are disabled to reduce the likelihood of vulnerabilities. All default network and security configurations are secure. Each factory default password is either set to a unique value during production or is required be changed by the user on first use.	• CR 1.5 Authenticator management • CR 7.6 Network and security configuration settings
8.10 Information deletion	
8.10-CO2 Personal information deletion: The charging station can securely erase sensitive information when no longer required to comply with privacy regulations such as the GDPR	• CR 4.2 Information persistence

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 analysed to detect incidents. <i>Remark:</i> 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 can be updated through remote access from the CPO central system. The local controller can check the authenticity of firmware or software through digital signatures. <i>Remark:</i> The local controller is the part that communicates with the CPO central system over the WAN. It is not required that other components of the charging station or plaza that are not reachable over the WAN can be remotely updated. It is however recommended to support remote updates for them to allow vulnerabilities in them to be patched more efficiently.	• CR 1.8 Public key infrastructure certificates • CR 1.9 Strength of public key-based authentication • EDR 3.10 Support for updates • EDR 3.10 RE1 Update authenticity and integrity • EDR 3.12 Provisioning supplier roots of trust • CR 4.3 Use of cryptography
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 3.5 Input validation • CR 7.1 Denial-of-service protection
8.22 Segregation of networks	
8.22-CO2 Logical network segregation on the charging station WAN: The charging station is segregated from other zones on the WAN interface. The charging station only allows connections to the CSMS.	• NDR 5.2 Zone boundary protection • NDR 5.2 RE1 Deny all, permit by exception
8.24 Use of cryptography	
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. When the charging station generates passwords or keys it should ensure that they are long and complex enough to be resistant against brute-force attacks	• CR 1.5 Authenticator management • CR 1.7 Strength of password-based authentication • CR 1.8 Public key infrastructure certificates • CR 1.9 Strength of public key-based authentication • EDR 3.13 Provisioning asset owner roots of trust

Annex 1 – Requirements for a direct supplier connection

As stated in section 2.1.2, when selecting the alternative remote maintenance method for the EV charging stations, additional security objectives and requirements apply. Annex 1 defines the additional users to the charging station, security objectives, and requirements that must be taken into account when allowing for a direct supplier connection to the EV charging station.

A1.1 Users and access rights

Table 2 following table lists the additional users that are authorized to access the EV charging station, the access they require, and the interfaces they use.

Table 5 Additional user groups on the charging station.

User	Required access	Interface
Supplier maintenance system	- Remotely configure the charging station - Remotely restore the charging station from a backed-up configuration - Remotely update the firmware - Analyze the operational logs	WAN

This document assumes that the supplier uses a maintenance system and that role-based authentication for their engineers will be managed through this system. Additional requirements to the supplier's maintenance system for access control are described in A1.3.

A1.2 Additional requirements to the charging station

When allowing for a direct connection to the charging station supplier, additional objectives and requirements must be considered on top of the objectives and requirements defined in the main document.

A1.2.1 Additional objectives

The table below shows the additional component-level security objectives for a direct supplier connection and the corresponding security requirements from IEC 62443-4-2 selected.

Table 6 Breakdown of objectives for direct supplier connection into IEC 62443-4-2 requirements

Objectives	Requirements to the charging station
8.5 Secure authentication	
8.5-CO7 Secure access to supplier maintenance systems for remote maintenance: The charging station shall only establish remote maintenance connections with the supplier maintenance system. Access to these systems shall be restricted by the supplier to authorized personnel using individual accounts and multi-factor authentication. All remote-maintenance sessions shall be recorded and retained for at least 30 days. The records shall be provided to the CPO upon request.	• CR 1.2 Software process and device identification and authorization • CR 1.2 RE1 Unique identification and authentication • CR 2.1 RE1 Authorization enforcement for all users (humans, software processes and devices) • CR 2.8 Auditable events • CR 2.9 Audit storage capacity • CR 2.12 Non-repudiation
8.20 Network security	
8.20-CO4 Controlled connection to manufacturer systems: The charging station may establish a connection to systems operated by the manufacturer only after the connection has been explicitly enabled by the CPO through the CSMS. The connection is disabled by default and can be enabled or disabled by the CPO at any time.	• NDR 1.13 Access via untrusted networks • NDR 1.13 RE1 Explicit access request approval • CR 2.6 Remote session termination
8.22 Segregation of networks	
8.22-CO3 Logical network segregation on the charging station WAN: The charging	• NDR 5.2 Zone boundary protection

station is segregated from other zones on the WAN interface. The charging station only allows connections to the CSMS and the supplier maintenance system when enabled.	NDR 5.2 RE1 Deny all, permit by exception
---	---

A1.2.2 Security requirements

The table below lists the additional requirements selected or applicable from the IEC 62443-4-2 standard on *Technical security requirements for IACS components* [1] or applicable contextualizations when the direct supplier connection is selected.

Table 7 Additional security requirements for direct supplier connection method

IEC	Name
CR 1.2 RE1	Unique identification and authentication <i>Contextualization – unique authentication for the supplier maintenance system:</i> The component shall provide the capability to uniquely identify and authenticate itself to the supplier maintenance system, and to enforce that the supplier maintenance system uniquely identifies and authenticates itself to the component before giving it access.
CR 2.1 RE1	Authorization enforcement for all users (humans, software processes and devices) <i>Contextualization – separation of roles:</i> The component shall provide the capability to separate, besides the roles defined in section 2.3, the role of the supplier maintenance system.
NDR 1.13	Access via untrusted networks
NDR 1.13 RE1	Explicit access request approval <i>Contextualization – access enabled by CPO:</i> the charging station shall allow administrators from the CPO to disable and enable the connection from the charging station to the suppliers' maintenance system.
CR 2.12	Non-repudiation
NDR 5.2 RE1	Deny all, permit by exception <i>Contextualization – Connection allowed to the supplier maintenance system:</i> the component shall allow only connections to the charging station supplier's maintenance system when the connection is enabled by the CPO. <i>Implementation guidance:</i> An additional SIM card can be placed in the charging station for the connection with the supplier maintenance system. The SIM card shall be managed by the CPO. Note: When procuring a charging station with direct supplier connection, the contextualization and implementation guidance of NDR 5.2 RE1 in the main document must be replaced with this contextualization and implementation guidance.

A1.3 Requirements to the supplier maintenance system

If the charging station allows a direct connection to the supplier, additional system requirements should be placed on the supplier's maintenance system in order to ensure secure access by the supplier engineers to the charging stations.

This section includes a non-exhaustive list of security requirements according to IEC 62443-3-3 standard on *Technical security requirements for IACS systems* [22] that the supplier maintenance system should follow to support objective 8.5-CO7 to the charging station. It is recommended that the supplier follows an ISMS that covers the supplier maintenance system, such as ISO/IEC 27001 or IEC 62443-2-1.

Table 8 Breakdown of objectives into IEC 62443-3-3 requirements

Objective	Requirements to the supplier maintenance system
8.5 Secure authentication	
8.5-CO7 Secure access to supplier maintenance systems for remote maintenance: The charging station shall only establish remote maintenance connections with the supplier maintenance system. Access to these systems shall be restricted by the supplier to authorized personnel using individual accounts and multi-factor authentication. All remote-maintenance sessions shall be recorded and retained for at least 30 days. The records shall be provided to the CPO upon request.	• SR 1.1 Human user identification and authorization • SR 1.1 RE1 Unique identification and authentication • SR 1.1 RE2 Multifactor authentication for untrusted networks • SR 2.1 RE1 Authorization enforcement for all users (humans, software processes and devices) • SR 2.8 Auditable events • SR 2.8 RE1 Centrally managed, system-wide audit trail • SR 2.9 Audit storage capacity • SR 2.11 Timestamps • SR 2.11 RE1 Internal time synchronization • SR 2.11 RE2 Protection of time source integrity • SR 2.12 Non-repudiation

The table below lists the requirements selected or applicable from the IEC 62443-3-3.

Table 9 Security requirements selected or are applicable from IEC 62443-3-3

IEC	Name
SR 1.1	Human user identification and authentication
SR 1.1 RE1	Unique identification and authentication
SR 1.1 RE2	Multifactor authentication for untrusted networks <i>Contextualization – multifactor authentication for supplier’s engineers:</i> The control system shall provide multifactor authentication for engineers on the supplier maintenance system. Best practices such as the ones published by NIST [15] must be followed.
SR 2.1 RE1	Authorization enforcement for all users <i>Contextualization – Separation of roles:</i> The control system shall provide the capability to separate roles to implement the principle of least privilege. Only the role of engineer shall be able to access remotely the EV charging stations.
SR 2.8	Auditable events <i>Contextualization – Session recording:</i> The control system shall provide the capability to record user sessions, including user identity, login and logout time, source, and security-relevant activities performed during the session.
SR 2.8 RE 1	Centrally managed, system-wide audit trail
SR 2.9	Audit storage capacity <i>Contextualization – sufficient resources:</i> The control system shall have enough resources to allow recorded events to be saved for at least 30 days.
SR 2.12	Non-repudiation

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
TLS	Transport Layer Security
WAN	Wide Area Network

References

- [1] ISA / IEC, "ISA 62443-4-2 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components," 2019.
- [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] ENCS, "EV-111-2022 Threat analysis for EV charging infrastructure," 2022.
- [4] IEC, "IEC 62443-1-5: Rules for IEC 62443 profiles," 2022.
- [5] European Commission, Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e), (c), 2022.
- [6] ENCS, EV-211-2022: IEC 62443 security requirements for EV charging infrastructure, 2022.
- [7] ENCS, "EV-312: Implementing IEC 62443-4-2 requirements in OCPP 2.0.1," 2025.
- [8] ENCS, "EV-313: Coverage of EN 18031 requirements by the IEC 62443 requirements for EV charging stations," 2025.
- [9] Elaad NL, Public Key Infrastructure for ISO 15118 - Freedom of choice for consumers & an open access market, 2022.
- [10] 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.

- [11] 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.

- [12] DIN, "DIN SPEC 70121 Electromobility - Digital communication between a d.c. EV charging station and an electrical vehicle for control of d.c. charging in the Combined Charging System," 2014.

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

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

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

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

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

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

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

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

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