EV-211

Security requirements from IEC 62443 for EV charging infrastructure

Version 2025v1.1

10 October 2025

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 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

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	Versions	Description
April 2016	EV-201-2016 v1.0	EV Charging Systems Security – D1.1 Architecture
December 2019	EV-201-2019 v1.0	Security architecture for electric vehicle charging infrastructure
February 2025	EV-211 2025v1.0	EV charging infrastructure security requirements based on the security architecture EV-111 with ISO 27002:2022 objectives.
October 2025	EV-211 2025v1.1	Fix of inconsistencies in the document

ENCS

Table of Contents

1 Introduction

This document gives security requirements that Charge Point Operators (CPOs) can use when procuring new EV charging infrastructures from a system integrator, or internally when designing and implementing an EV charging infrastructure. The requirements are based on the IEC 62443 standard. They have been selected from *IEC 62443-3-3: System security requirements and security levels* [1].

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

However, this also means that CPOs are a target for cyber-attacks. If attackers gain control of a CPO's infrastructure, they could switch the power on the connected charging stations. Such an attack would not only hurt the CPOs themselves. The switching could also cause grid imbalances in the supply and demand for electricity and, possibly, power outages. If smart charging is used, attackers may force charging stations to use more power than assigned to them, which could damage transformers and power lines.

Making sure the EV charging infrastructure is secure is, hence, critical. This document provides a recommended set of security requirements at a system level that allows the major security threats to be mitigated with current technology. It provides guidance on what organizational and technical measures to take to secure EV charging infrastructures.

The requirements can be used by local governments procuring charging services from a CPO to ensure that these services are delivered securely. They can also be used internally by a CPO to determine how to secure their own systems.

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 [2] they form a profile for IEC 62443 (following the rules in [3]).

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* [2] 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 [4].

- *EV-311: Security requirements from IEC 62443 for procuring EV charging stations* [5] contains security requirements that CPOs can use when they procure EV charging stations. The requirements are chosen so that a charging station meeting them can be easily integrated into a system meeting the security requirements in this document.
- *EV-312: Implementing IEC 62443-4-2 requirements in OCPP 2.0.1* [6] provides guidance on how the requirements in this EV-311 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* [7] shows how the requirements in the harmonized standard EN 18031 for the Radio Equipment Directive are covered by the requirements in EV-311.

2 System description

To effectively use the security requirements, it is important to know the assumptions they make about how the EV charging infrastructure works. This includes the intended use of the system, its operational environment, and the zoning model and access control model used in the threat analysis [2] to set security objectives.

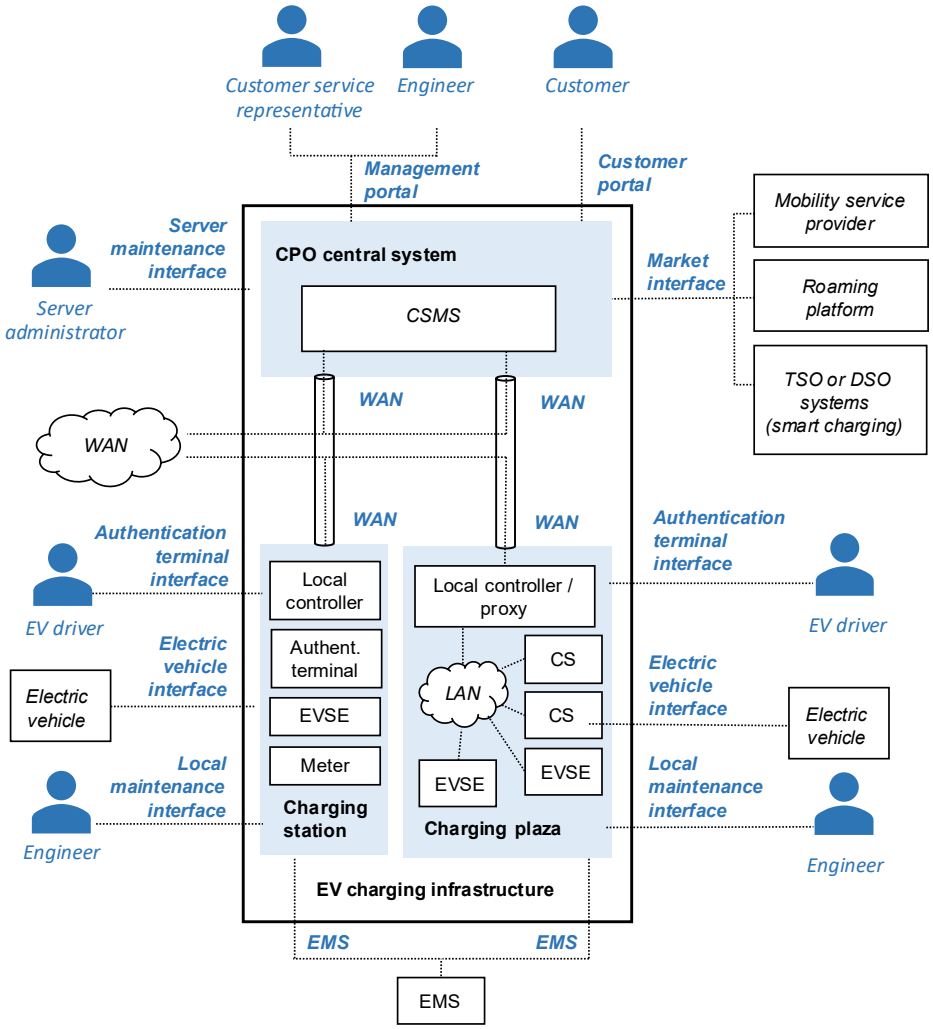

Figure 1: Reference architecture for the EV charging infrastructure, showing its users and interfaces.

2.1 Intended use of the system

The EV charging infrastructure consists of the systems used by a Charge Point Operator (CPO) to operate and maintain their charging stations and plazas. This includes the charging stations themselves, and the central systems such as the charging station management system (CSMS).

2.1.1 Components in the system

The CPO central system manages the different charging stations through the charging station management system (CSMS). It contains the servers and workstations used to maintain the CPOs charging stations remotely.

The central system allows to exchange information with mobility service providers and roaming platforms to allow EV drivers to use charging stations operated by different CPOs.

In some cases, the central system also connects to the systems of a Transmission System Operator (TSO) or Distribution System Operator (DSO) to allow smart charging. The rate of charging is then adjusted based on the capacity of the electricity grid.

Through the customer portal, customers can retrieve their transaction data and contact customer services, who can access the CPO central system through the management portal, like engineers, to solve issues for the customers. The customer portal is not in the scope of this document. However, it should be developed following secure development guidelines.

The charging stations can be standalone devices or be in a group forming a charging plaza. The charging stations usually include a local controller and authentication terminal for EV drivers to authenticate to the device, the electric vehicle supply equipment (EVSE) to supply electrical power to the EV vehicles, and a meter, to measure how much power is supplied. The charging station can also be locally maintained by engineers.

2.1.2 Users of the system

The CPO central system is maintained by employees or contractors of the charge point operator. This document distinguishes between three different groups:

- **Customer service representatives** working for instance at the helpdesk of the CPO. They assist customers with simple problems with the charging stations and have limited access to the central system.
- **Engineers** that maintain the charging stations. They can make changes to the charging station configuration and update the firmware.
- **Server administrators** that maintain the CPO central system. They are responsible for both the server infrastructure, such as operating systems, virtualization platforms, databases, and CSMS applications.

The charging stations themselves can be accessed by electric vehicle drivers to start and stop charging. Electric vehicles themselves communicate with the charging station to, for instance, control the charging speed and to stop charging when the vehicle’s battery is full.

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

Table 1 lists the interfaces through which the EV charging infrastructure is connected to the operational environment.

Table 1 Interfaces connecting the EV charging infrastructure to the operational environment.

Interface	Description
Management portal	Customer service representatives and engineers can access the CPO central system through the management portal to get information on charging stations and change their state or configuration. The management portal is usually a web portal accessed over the internet.
Customer portal	Customers can access their customer and billing information through the customer portal. The customer portal can be a web portal on the internet or a smartphone app.
Market	The central systems are connected to the market parties, such as mobility service providers, roaming platforms, and DSO and TSO systems, over the market interface. The connections are usually over the internet, sometimes through a VPN. Typically, web services are used, for instance using the OCPI, OCHP, OSCP, and OICP protocols [8].
Server maintenance	Server administrators the server maintenance interface to perform maintenance on the CPO central system servers. The interface is usually accessed over the internet, sometimes through a VPN. Administrators can use any protocol used to administer servers, such as remote desktop protocols or SSH.
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).
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 [8]. 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

The CPO central system can be located in the data centres of the CPO or a cloud system.

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 Zoning model

In the reference architecture (Figure 1), the EV charging infrastructure is divided into three zones:

- The **CPO central system** consists of all servers that are used to manage and maintain the charging stations remotely.
- The **charging station** consists of all the equipment physically inside the charging station. This can include a local controller, the authentication terminal, the electric vehicle supply equipment (EVSE), and a meter.
- The **charging plaza** consists of all EV charging equipment in a charging plaza connected to the central system through one local controller or proxy. This can include multiple charging stations and EVSE, and a local area network (LAN).

The zoning model allows to set different objectives for the different types of systems in each zone. The CPO central system is a modern IT application, often running in the cloud. The charging station is an embedded system, usually placed in public locations without supervision. The charging plaza consists of multiple embedded systems, connected over a local network in a somewhat supervised location. Different security measures can and should be taken for each type of system. Technical objectives for the charging station and plaza are the same, whereas the physical objectives differ.

2.4 Access control policy

To determine what access control measures have to be taken in each zone, we need to know the users of the zone Table 2 and Table 3 list the users that are authorized to access the CPO central system and the charging station and plaza respectively, and the access they require. The last column gives the interfaces on which they access the system (see the reference architecture in Figure 1).

Table 2 User groups on the CPO central system.

User	Required access	Interface

Charging station	• Send transaction data and meter values for billing • *Optional:* Get charging profiles	WAN
Engineers	• Remote maintenance to charging stations through the central system	Management portal
Customer service representative	• Fix customer problems with charging stations	Management portal
Customers	• See transaction information	Customer portal
Market parties (mobility service provider, roaming platform, TSO, or DSO)	• Exchange transaction data • Enable EV drivers to use charging stations from different CPOs • Provide smart charging schedules	Market interface
Server administrator	• Maintain applications • Maintain network and server infrastructure	Server maintenance interface

The access control model assumes that engineers do not access charging stations directly over the WAN. They always work through the central maintenance system.

Table 3 User groups on the charging station and charging plaza.

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	WAN

	• Optional: Send charging profiles	
Engineer	• Configure the charging station • Restore the charging station from a backed-up configuration • Update the firmware • Analyse 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 station	• Load balancing within a charging plaza	LAN
Local EMS	• Energy management within the local context (e.g., building)	LAN

3 Security requirements

This section gives the security requirements for procuring EV charging services. They include process requirements for the charge point operator, that follow the ISO/IEC 27002:2022 controls, and technological requirements for the EV charging infrastructure selected from the IEC 62443-3-3 standard on *System security requirements and security levels* [1]. The requirements were selected to cover the security objectives derived from the threat analysis [2], as further explained in Section 4.

Process controls that apply to the CPO are given in Section 3.1. Technological requirements that apply to the CPO central system in Section 2.3 are given in Section 3.1. Technological requirements for the charging station are given in Section 3.3.

3.1 Process requirements

Table 4 lists the security requirements for the security processes at the CPO. The requirements assume that the CPO has a management system based on ISO/IEC 27001 and implements certain controls from ISO/IEC 27002. On top of these controls, it includes specific requirements needed to offer secure EV charging services.

We use the term *"purchasing party"* for the party that purchases the EV charging services from the CPO.

Table 4: Security requirements for the CPO security processes.

Identifier	Requirement
OR 1	**Information security management system** The CPO shall have an information security management system meeting the requirements of ISO/IEC 27001 and covering the full EV charging system and its management processes. *Implementation guidance:* It is recommended that the system is certified against ISO/IEC 27001. The requirements below give mandatory controls from ISO/IEC 27002 to implement. CPOs should however also consider the other controls and implement them if they are needed to mitigate risks.
OR 2	**Access control processes**

Identifier	Requirement
	The CPO shall have a process to manage user's identities, accounts, and access rights, implementing the following controls from ISO/IEC 27002: • 5.15 Access control 5.16 Identity management 5.18 Access rights The CPO shall use personal accounts for all users on the management and customer portal.
OR 3	**Supplier management** The CPO shall have processes to manage the security of its suppliers, implementing the following controls from ISO/IEC 27002: • 5.19 Information security in supplier agreements • 5.20 Addressing information security within supplier agreements • 5.21 Managing information security in the ICT supply chain • 5.24 Information security incident management planning and preparation The CPO shall ensure that the technical requirements in Sections 3.2 and 3.3 are implemented by the suppliers of the charging stations, charging plazas, and central systems. The CPO shall, if requested, deliver test and audit reports showing that the requirements have been implemented. The CPO shall require that suppliers of the charging station, charging plazas, and central system have a vulnerability handling process and deliver security updates in a timely manner. The CPO shall require that suppliers of charging stations and charging plazas implement the following physical security measures: • The charging station or plaza sends an alert to the CSMS when any part of its casing or housing is opened. • 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. • The local controller or proxy in a charging plaza, and the networking equipment for a charging plaza will be placed in a locked cabinet. The cabinet protects against physical

Identifier	Requirement
	manipulation so that attackers without specialist tools cannot reach its internal components without leaving visible traces. • 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. • The network cables of the charging plaza local area network and the connection to an EMS are protected against tampering. Attackers without specialist tools cannot physically connect to the corresponding interfaces without leaving visible traces. *Supplemental guidance:* Supplier agreements between the CPO and their suppliers should ensure that the CPO can meet the other requirements in this section, including those for security events, incident handling, and vulnerability handling. When CPOs use the technical requirements in this document, it is recommended to also require that any software supplier complies fully with **IEC 62443-4-1** [13] and any system integrator complies fully with **IEC 62443-2-4** [14] both at **a maturity level of at least 3**. Doing so ensures that the supplier has secure development processes, so that it can correctly and consistently implement the technical requirements described in the following sections. The scope of application of the standards should cover the software developed for the charging infrastructure and all systems the supplier is responsible for.
OR 4	**Security event and incident handling** The CPO shall have processes to monitor security events and respond to security incidents, implementing the following controls from ISO/IEC 27002: • 5.25 Assessment and decision on information security events • 5.26 Response to information security incidents • 8.15 Logging • 8.16 Monitoring activities The CPO shall report security incidents in its EV charging system to the purchasing party.

Identifier	Requirement
	The CPO shall collect the security logs of the charging stations and central systems centrally and define risk-based use cases to monitor for incidents. *Implementation guidance:* Procedures, rules, and use cases should be defined to find incidents in SIEM logs. A process should be established to respond to the incidents and minimize the impact.
OR 5	**Business continuity** The CPO shall ensure business continuity of the EV charging infrastructure, implementing the following controls from ISO/IEC 27002: • 5.30 ICT readiness for business continuity • 8.14 Redundancy of information processing facilities The CPO shall ensure that charging transactions can be completed even when one of the data centres hosting the central systems is disrupted by a natural disaster or power outage.
OR 6	**Protecting personal information** The CPO shall protect the personal information of customers and employees, implementing the following controls from ISO/IEC 27002: • 5.34 Privacy and protection of PII • 8.10 Information deletion • 8.11 Data masking *Implementation guidance:* A process should be defined to remove sensitive information stored in the charging stations when no longer required. The CPO can define a period for data retention subject to regulations and internal policies. A policy should be defined to ensure that sensitive data stored in charging stations is protected by hiding techniques such as data masking, pseudonymization, or anonymization.
OR 7	**Personnel security** The CPO shall implement personnel security processes covering the following controls from ISO/IEC 27002:2022:

Identifier	Requirement
	• 6.1 Screening • 6.2 Terms and conditions of employment • 6.3 Information security awareness, education, and training • 6.4 Disciplinary process • 6.5 Responsibilities after termination or change of employment
OR 8	**Physical security of the central systems** The CPO shall implement physical security processes for the central systems covering the following controls from ISO/IEC 27002:2022: • 7.1 Physical security perimeters • 7.2 Physical entry • 7.3 Securing offices, rooms, and facilities • 7.4 Physical security monitoring • 7.8 Equipment siting and protection • 7.12 Cabling security
OR 9	**Physical security of the charging stations** The CPO shall implement physical security processes for the charging stations covering the following controls from ISO/IEC 27002:2022: • 7.4 Physical security monitoring • 7.8 Equipment siting and protection • 7.12 Cabling security The CPO shall monitor physical security events on the charging stations and plazas and responds to them.
OR 10	**Vulnerability management process** The CPO shall have processes to manage vulnerabilities in the EV charging infrastructure, implementing the following controls from ISO/IEC 27002: • 8.8 Management of technical vulnerabilities *Implementation guidance:* The CPO should define a clear policy on when vulnerabilities must be patched, based on their severity. The CVSS score could be used as a severity measure but must usually be

Identifier	Requirement
	complemented with information about the location of the vulnerability in the system. The purchasing party should conclude a service level agreement (SLA) with the CPO on the delivery of patches. The SLA shall take into account the risk exposure of the interfaces. For example, if an APN is used to connect the CSMS and the charging station, the patching SLA might be longer than if that communication goes through an open mobile connection. An example of a prioritization ranking:

CVSS Score	Target SLA
1-3	Next patch cycle
4-6	1 month
7-8	2 weeks
9-10	As soon as possible

OR 11	**Backup process** The CPO shall have processes to back up both the central systems and the charging station configuration, implementing the following controls from ISO/IEC 27002: • 8.13 Information backup *Implementation guidance:* A process should be defined to back up the charging station and plaza configurations on the CPO central system. The backup integrity can be verified. Older versions of the configurations should be kept so that it is possible to revert to them in case of issues. There should be an automated process to back up the data and configurations on the CPO central systems.
OR 12	**Protecting networks** The CPO shall take measures to mitigate security risks on the networks that it uses, implementing the following controls from ISO/IEC 27002: • 8.20 Network security

Identifier	Requirement
	• 8.21 Security of network services • 8.22 Segregation of networks The CPO shall ensure that charging stations cannot be reached directly from the Internet. The CPO shall ensure that the wide-area network (WAN) is resilient against accidental disruptions and against intentional denial-of-service attacks using simple means with low resources, generic skills, and low motivation. The CPO shall ensure that it is not possible to have direct communication between charging stations on the WAN network. The charging stations shall only be allowed to communicate with the CPO central system. *Implementation guidance:* The CPO should agree on the required service level for the WAN with the telecom provider and is regularly monitored. The telecom provider monitors the network and can respond in case of an incident to minimize the impact of attacks. The internet connections for the management portal and market interfaces are resilient against accidental disruptions and intentional denial-of-service attacks using simple means with low resources, generic skills, and low motivation (security level 2). The required service level is agreed with the telecom provider and is regularly monitored. The telecom provider monitors the network and can respond in case of an incident to minimize the impact of attacks.
OR 13	**Key and password management process** The CPO shall have a process for key management, implementing the following controls from ISO/IEC 27002: • 8.24 Use of cryptography The CPO shall have a process to periodically update the keys on the EV charging stations. *Implementation guidance:* To meet requirement SR 1.2 below, charging stations must use unique keys or passwords to authenticate to the CSMS. The CPO should ensure that such keys are installed on the charging station immediately after installation and provisioning.

Identifier	Requirement
	Preferably, charging stations are already delivered by the manufacturer with unique and secure passwords and keys. Even in that case, it is recommended to change the keys after provisioning to limit the risk of keys being compromised at the charging station manufacturer.

3.2 Requirements applicable to the CPO central system

Table 5 below lists the requirements from IEC 62443-3-3 [1] that apply to the CPO central system. Following the convention in IEC 62443-3-3, the adaptations and supplemental guidance use the term *'control system'* for the CPO central system.

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 the contextualization within the requirements must be followed. They 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.

Besides the contextualization, **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.

Table 5 Full list of requirements selected from IEC 62443-3-3 for the CPO central system

IEC identifier	Name
SR 1.1	**Human user identification and authentication**
SR 1.1 RE 1	**Unique identification and authentication**
SR 1.1 RE2	**Multifactor authentication for untrusted networks** *Contextualization – multifactor authentication for server administrators:* The control system shall provide multifactor authentication for server

IEC identifier	Name
	administrators on the server maintenance interface. Best practices such as the ones published by NIST [15] must be followed.
SR 1.2	**Software process and device identification and authentication** *Contextualization – authentication on all interfaces:* The control system shall provide the capability to identify and authenticate the role of the charging stations, mobility service provider, roaming platform, and DSO systems. This capability shall enforce such identification and authentication on all interfaces that provide access to the components to support the least privilege in accordance with applicable security policies and procedures. Devices in the control system uniquely identify themselves to the CPO central system and allow the system to authenticate them. *Implementation guidance:* When validating a certificate, the role of the user can be checked through the subject name, common name, or distinguished name.
SR 1.2 RE1	**Unique identification and authentication**
SR 1.3	**Account management** *Contextualization – account creation on customer portal:* The control system shall allow customers to create new accounts on the customer portal. *Contextualization - account creation on management portal:* The control system shall only allow server administrators to create accounts for engineers and customer representatives on the management portal.
SR 1.3 RE1	**Unified account management** *Contextualization – centralized account management*: The control system shall provide the capability to be integrated into a central access control system for managing the accounts of all human users. The component shall assign an account to a role based on information from the central access control system.

IEC identifier	Name
	Implementation guidance: The central system can check a user's access rights using different technologies. CPOs should choose a method that works with their existing systems.
SR 1.4	**Identifier management**
SR 1.5	**Authenticator management** *Contextualization – authenticator updates over the server maintenance interface:* The control system shall provide server administrators the capability to update all authenticators over the server maintenance interface. It shall be possible to update them without support from suppliers. The confidentiality and integrity of the authenticators shall be protected during changes. *Contextualization – authenticator updates for the customer portal*: The control system shall provide customers on the customer portal with the capability of managing their accounts. Customers shall be able to change and recover passwords. For customer representatives and engineers' accounts on the management portal, the server administrators shall perform any authenticator change. *Contextualization – password storage:* The control system shall at least provide the capability to protect passwords from unauthorized disclosure by storing them salted and hashed. *Implementation guidance:* The contextualization only concerns point c) and part of point d) of the original requirement. The rest of the requirement stays in force without adaptation. For storing passwords, it is recommended to use a hashing function that is resistant to GPU cracking attacks, such as Argon2 or PBKDF2.
SR 1.7	**Strength of password-based authentication** *Implementation guidance:* It is recommended that users follow a secure password policy, such as the one described in the guidance of control 5.17 of the ISO 27002 [16]

IEC identifier	Name
SR 1.7 RE1	**Password generation and lifetime restriction for human users**
SR 1.8	**Public key infrastructure certificates**
SR 1.9	**Strength of public key-based authentication**
SR 1.10	**Authenticator feedback**
SR 1.11	**Unsuccessful login attempts**
SR 2.1	**Authorization enforcement** *Contextualization – switching restriction:* The control system shall be able to restrict on how many charging stations a user can control charging operations in a time period. *Implementation guidance:* The restrictions should at least ensure that users cannot switch charging on or off on many charging stations at the same time. The control system should be limited to how many charging stations a switching command can be sent and how many commands can be sent per hour.
SR 2.1 RE1	**Authorization enforcement for all users** *Contextualization – **Separation of roles**:* The control system shall provide the capability to separate the following roles to implement the principle of least privilege: • Charging station • Engineers • Customer representative • Customers • Market parties • Server administrator *Implementation guideline:* For more information, refer to the access control policy described in Table 2 in Section 2.4.

IEC identifier	Name
SR 2.1 RE2	**Permission mapping to roles**
SR 2.5	**Session lock**
SR 2.6	**Remote session termination**
SR 2.8	**Auditable events**
SR 2.8 RE 1	**Centrally managed, system-wide audit trail**
SR 2.9	**Audit storage capacity**
SR 2.10	**Response to audit processing failures**
SR 2.11	**Timestamps**
SR 2.11 RE1	**Internal time synchronization**
SR 2.11 RE2	**Protection of time source integrity**
SR 3.1	**Communication integrity**
SR 3.1 RE1	**Cryptographic integrity protection** *Contextualization* – ***Authentication of WAN communication****:* The control system shall provide the capability to verify the authenticity of information received on the WAN, management portal, market interface, and server maintenance interfaces using cryptographic methods.
SR 3.2	**Malicious code protection**

IEC identifier	Name
	Contextualization – ***Active malware protection****:* Hosts running commercial off-the-shelf operating systems shall have the capability to actively detect and respond to malware. ***Software and hardware security features***: All hosts shall allow security features available on the hardware and software platforms to be enabled. ***Management from server maintenance interface:*** Server administrators shall be able to manage malware detection and response and the security features from the server maintenance interface. *Implementation guidance:* Detection and response to malware may for instance be provided through anti-virus software, endpoint protection, or application whitelisting. It is recommended to use the following hardware features when they are supported: • *No-Execute (NX) / Write-xor-execute (W^R):* A Memory Protection Unit (MPU) or Memory Management Unit (MMU) shall be used to mark code regions as read-only and data sections as non-executable. • *Address Space Layout Randomization (ASLR):* A Memory Management Unit (MMU) shall be used to load data and code at different memory addresses every time an application is run. The software running on the device must be compiled to use the hardware features. The Position Independent Code (PIC) or Position Independent Executable (PIE) compiler options should be enabled to be able to use ASLR. At the operating system layer, the user's access to filesystems should be minimized, and processes should be run with minimum privileges. Host-based firewalls should be enabled.
SR 3.4	**Software and information integrity**
SR 3.8	**Session integrity**
SR 3.9	**Protection of audit information**

IEC identifier	Name
SR 4.1	**Information confidentiality**
SR 4.1 RE1	**Protection of confidentiality at rest or in transit via untrusted networks** *Contextualization – encryption on the WAN:* The control system shall support the protection of the confidentiality of information in transit on the WAN, management portal, market interface, and server maintenance interfaces using encryption. Information at rest may be protected by access control mechanisms and physical protection. Cryptographic protection is not required for the information at rest. *Contextualization – data masking:* The control system shall support the confidentiality of sensitive data (special categories of personal data according to GDPR) through the use of data masking techniques. *Implementation guidance*: Data masking techniques include, but are not limited to, randomization, substitution, and encryption.
SR 4.1 RE2	**Protection of confidentiality across zone boundaries**
SR 4.2	**Information persistence** *Contextualization – personal data deletion:* The control system shall allow for personal data in the CSMS and stored on the charging stations to be deleted after a certain retention period. The control system shall also allow customers to delete their personal data.
SR 4.3	**Use of cryptography** *Implementation guidance:* 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 *Cryptographic Mechanisms: Recommendations and Key Lengths* [19]

IEC identifier	Name
	• the ECRYPT – *Algorithms, Key Size, and Protocols Report* [20] • the NIST *Recommendation for key management* [21] 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.
SR 5.1	**Network segmentation**
SR 5.2	**Zone boundary protection**
SR 5.2 RE 1	**Deny by default, allow by exception**
SR 6.1	**Audit log accessibility**
SR 6.1 RE 1	**Programmatic access to audit logs** *Implementation guidance:* The control system shall provide the capability to send the audit records using the syslog communication protocol in a commonly used format so that they can be easily imported into a SIEM system without the need for a customized parser.
SR 7.1	**Denial-of-service protection**
SR 7.1 RE1	**Manage communication loads**
SR 7.3	**Control system backup** *Contextualization – automated backups:* The control system supports making automated backups of all configurations and data on the system.

IEC identifier	Name
SR 7.3 RE1	**Backup verification**
SR 7.3 RE2	**Backup automation**
SR 7.4	**Control system recovery and reconstitution**
SR 7.6	**Network and security configuration settings** *Contextualization – configuration management over the server maintenance interface:* The control system allows administrators to manage and monitor the network and security configurations over the server maintenance interface.
SR 7.7	**Least functionality**

3.3 Requirements applicable to the charging stations and charging plazas

Table 6 below lists the requirements from the IEC 62443-3-3 standard on *System security requirements and security levels* [1] that apply to charging stations and charging plazas. Following the convention in IEC 62443-3-3, the adaptations and supplemental guidance use the term *'control system'* for the charging stations and charging plazas.

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 the contextualization within the requirements must be followed. They 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.

Besides the contextualization, **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.

Table 6 Full list of requirements selected from IEC 62443-3-3 for charging stations and charging plazas.

IEC identifier	Name
SR 1.1	**Human user identification and authentication** *Contextualization – Authentication for engineers:* The control system shall provide the capability to identify and authenticate the role of human users. *Contextualization – authentication for EV drivers:* The system shall identify and authenticate EV drivers on the authentication terminal using a mechanism chosen by the mobility service provider
SR 1.2	**Software process and device identification and authentication** *Contextualization – authentication on all interfaces:* The control system shall provide the capability to identify and authenticate the role of the CSMS, electric vehicle, engineers, EMS, and other charging stations.
SR 1.2 RE1	**Unique identification and authentication** *Contextualization – unique authentication for the CSMS:* The control system 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. *Contextualization – unique authentication for the electric vehicles:* If the control system is exchanging data with electric vehicles (for instance using the IEC 15118 protocol), it shall provide the capability to uniquely identify and authenticate itself to the electric vehicles, and to enforce that the electric vehicle uniquely identifies and authenticates itself to the component before giving it access. *Implementation guidance:* 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.
SR 1.5	**Authenticator management**

IEC identifier	Name
	Contextualization – authenticator updates from the CSMS: The control system shall provide the capability to automatically update all authenticators from the CSMS 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. *Contextualization - password storage*: The control system shall at least provide the capability to protect passwords from unauthorized disclosure by storing them salted and hashed. *Contextualization – factory default passwords:* If a factory default password is used for an authentication mechanism required by SR 1.1 or SR 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. *Implementation guidance:* The contextualization only concerns point c) and part of point d) of the original requirement. The rest of the requirement stays in force without adaptation. 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.
SR1.7	**Strength of password-based authentication**
SR 1.8	**Public key infrastructure certificates**
SR 1.9	**Strength of public key-based authentication**
SR 2.1	**Authorization enforcement**

IEC identifier	Name
SR 2.1 RE1	**Authorization enforcement for all users** *Contextualization – separation of roles:* The control system shall provide the capability to separate the following roles to implement the principle of least privilege: • CSMS • Engineer • EV driver • Electric vehicles • Other charging stations • EMS *Implementation guideline:* For more information, refer to the access control policy described in Table 3 in Section 2.4.
SR 2.6	**Remote session termination**
SR 2.8	**Auditable events**
SR 2.9	**Audit storage capacity**
SR 2.10	**Response to audit processing failures**
SR 2.11	**Timestamps**
SR 2.11 RE1	**Internal time synchronization**
SR 2.11 RE2	**Protection of time source integrity**
SR 3.1	**Communication integrity**
SR 3.1 RE1	**Cryptographic integrity protection**

IEC identifier	Name
	Contextualization – authentication of WAN communication: The control system shall provide the capability to verify the authenticity of information received on the WAN using cryptographic methods.
SR 3.2	**Malicious code protection** *Contextualization – hardware security features:* The control system shall be delivered with the security features from the underlying hardware and operating system enabled whenever possible.
SR 3.4	**Software and information integrity** *Contextualization – signed firmware and software updates:* Equipment in the control systems 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. *Implementation guidance:* It is not required that the integrity or authenticity of the firmware or software is validated during boot ("secure boot").
SR 3.5	**Input validation** *Contextualization – no known vulnerabilities:* The control system 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 *Contextualization – testing for input validation vulnerabilities:* 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.
SR 3.9	**Protection of audit information**
SR 4.1	**Information confidentiality**

IEC identifier	Name
SR 4.1 RE1	**Protection of confidentiality at rest or in transit via untrusted networks** *Contextualization – encryption of WAN communication:* The control system shall support the protection of the confidentiality of information in transit on the WAN interface using encryption. I *Contextualization - protection of information at rest*: Information at rest may be protected by access control mechanisms and physical protection. Cryptographic protection is not required at rest.
SR 4.1 RE2	**Protection of confidentiality across zone boundaries**
SR 4.2	**Information persistence** *Contextualization – deletion of personal:* the control system shall be able to delete any personal information stored in it on request of the CSMS. *Implementation guidance:* Transaction information and charging authorizations could include information used to identify individual EV users. Such information should be considered personal data.
SR 4.3	**Use of cryptography** *Implementation guidance:* 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 *Cryptographic Mechanisms: Recommendations and Key Lengths* [19] • the ECRYPT – *Algorithms, Key Size, and Protocols Report* [20] • the NIST *Recommendation for key management* [21] The latest version of these reports should be followed.

IEC identifier	Name
	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.
SR 5.1	**Network segmentation**
SR 5.2	**Zone boundary protection** *Contextualization – firewalling on WAN interface:* The control system shall apply firewall functionality to monitor and control communication on the WAN interface. *Implementation guidance:* For stand-alone charging stations, the firewall is usually implemented in the integrated telecom modem. For charging plazas, the firewall could also be implemented in a separate modem or firewall.
SR 5.2 RE1	**Deny by default, allow by exception**
SR 6.1	**Audit log accessibility**
SR 6.1 RE1	**Programmatic access to audit logs** *Contextualization – audit logs collected by CSMS: The control system* shall allow the CSMS to collect security events.
SR 7.1	**Denial-of-service protection** *Implementation guidance:* In the degraded mode, at least the charging functions should continue to work properly.
SR 7.1 RE1	**Manage communication loads**

IEC identifier	Name
SR 7.4	**Control system recovery and reconstitution** *Contextualization – restoration from CPO central system:* The control system shall have the capability to be restored from a backed-up configuration by the CPO central system.
SR 7.6	**Network and configuration settings** *Contextualization – secure configuration by default:* The control system shall be delivered by the manufacturer with the recommended network and security configurations.
SR 7.7	**Least functionality** *Contextualization – hardened by default*: The control system shall be delivered with all unneeded functions disabled. In particular, they 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.

4 Rationale for the requirements

The requirements in Section 3 have been chosen based on the security objectives derived in the threat analysis for EV charging infrastructure [2]. This section shows which the requirements cover these objectives.

4.1 Rationale for the process requirements

Table 7 shows how the requirements in Section 3.1 cover the security objectives for the operational environment.

Table 7: Coverage of the security objectives to the operational environment by the process requirements.

Security Objective	***IEC 62443-3-3 requirements***
5-SO1 Access control processes: The CPO has implemented access control processes covering the following controls from ISO/IEC 27002:2022: • 5.4 Management responsibilities • 5.9 Inventory of assets and other information • 5.15 Access control • 5.16 Identity management • 5.18 Access rights	• OR 2 Access control processes
5-SO2 Supplier management: The CPO has implemented processes to manage the security of its suppliers, covering the following controls from ISO/IEC 27002: • 5.19 Information security in supplier agreements • 5.20 Addressing information security within supplier agreements • 5.21 Managing information security in the ICT supply chain	• OR 3 Supplier management

• 5.24 Information security incident management planning and preparation	
5-SO3 Security event and incident handling: The CPO has implemented security event and incident handling processes covering the following controls from ISO/IEC 27002:2022: • 5.25 Assessment and decision on information security events • 5.26 Response to information security incidents	• OR 4 Security event and incident handling
5-SO4 Business continuity: The CPO has implemented business continuity policies and processes covering the following controls from ISO/IEC 27002:2022 • 5.30 ICT readiness for business continuity	• OR 5 Business continuity
5-SO5 Protecting personal information: The CPO has implemented a process to protect the privacy and personal information of its customers and employees covering the following controls from ISO/IEC 27002:2022: • 5.34 Privacy and protection of PII	• OR 6 Protecting personal information
6-SO1 Personnel security: The CPO has implemented personnel security processes covering the following controls from ISO/IEC 27002:2022: • 6.1 Screening • 6.2 Terms and conditions of employment • 6.3 Information security awareness, education, and training • 6.4 Disciplinary process	• OR 7 Personnel security

• 6.5 Responsibilities after termination or change of employment	
7-SO1 Physical security: The CPO has implemented a physical security policy covering the following controls from ISO/IEC 27002:2022: • 7.1 Physical security perimeters • 7.2 Physical entry • 7.3 Securing offices, rooms, and facilities • 7.4 Physical security monitoring • 7.8 Equipment siting and protection • 7.12 Cabling security	• OR 8 Physical security of the central systems • OR 9 Physical security of the charging stations
7.4-SO1 Physical access detection on charging stations: The charging station sends an alert to the CSMS when any part of its casing is opened.	• OR 3 Supplier management
7.4-SO2 Physical access detection on charging stations: The cabinets housing the charging plaza equipment (see objective 7.4-SO1) send an alert to the CSMS when they are opened.	• OR 3 Supplier management
7.4-SO3 Physical access monitoring: The charge point operator monitors physical security events on the charging stations and plazas and responds to them.	• OR 9 Physical security of the charging stations
7.8-SO1 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.	• OR 3 Supplier management
7.8-SO2 Tamper protection for charging plaza equipment: The local controller or	• OR 3 Supplier management

proxy, and the networking equipment for a charging plaza will be placed in a locked cabinet. The cabinet protects against physical manipulation so that attackers without specialist tools cannot reach its internal components without leaving visible traces.	
7.12-SO1 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.	• OR 3 Supplier management
7.12-SO2 Cabling security for charging plazas: The network cables of the charging plaza local area network and the connection to an EMS are protected against tampering. Attackers without specialist tools cannot physically connect to the corresponding interfaces without leaving visible traces.	• OR 3 Supplier management
8.8-SO3 Vulnerability management process: The charge point operator manages vulnerabilities in the system by: • disabling unused ports, services, user accounts, and functions to reduce the likelihood of vulnerabilities • monitoring vulnerabilities in the system's software and firmware, assessing the risks of the vulnerabilities, and mitigating the high-risk vulnerabilities, for instance by applying security updates • limiting the impact of vulnerabilities by enabling the security features on	• OR 10 Vulnerability management process

the hardware and software platforms used	
8.10-SO3 Personal information deletion process: The charge point operator has a process to remove sensitive information stored in the charging stations when no longer required.	• OR 6 Protecting personal information
8.11-SO2 Data masking policy: The charge point operator has a policy to ensure that sensitive data stored in charging stations is protected by hiding techniques such as data masking, pseudonymization, or anonymization.	• OR 6 Protecting personal information
8.13-SO2 Backup process for charging station configurations: The charge point operator has a process to back up the charging station and plaza configurations on the CPO central system. Older versions of the configurations are kept so that it is possible to revert to them in case of issues.	• OR 11 Backup process
8.13-SO3 Backup process for the CPO central system: The charge point operator has an automated process to back up the data and configurations on the CPO central systems (including the charging station and plaza configurations stored there according to 8.13-SO2).	• OR 11 Backup process
8.16-SO1: Security monitoring and incident response: The charge point operator monitors and responds to security events on the CPO central system and the charging stations and plazas. They gather security logs from the devices centrally, for instance, in a SIEM. They establish procedures, use cases, and rules to find incidents in the logs. And they establish a	• OR 4 Security event and incident handling

process for responding to the incidents and minimizing the impact.	
8.21-SO1 Resilience against denial-of-service attacks on the WAN: The wide-area network (WAN) is resilient against accidental disruptions and intentional denial-of-service attacks using simple means with low resources, generic skills, and low motivation. The required service level is agreed with the telecom provider and is regularly monitored. The telecom provider monitors the network and can respond in case of an incident to minimize the impact of attacks.	• OR 12 Protecting networks
8.21-SO2 Resilience against denial-of-service attacks on the internet-facing interfaces: The internet connections for the management portal and market interfaces are resilient against accidental disruptions and against intentional denial-of-service attacks using simple means with low resources, generic skills, and low motivation. The required service level is agreed with the telecom provider and is regularly monitored. The telecom provider monitors the network and can respond in case of an incident to minimize the impact of attacks.	• OR 12 Protecting networks
8.22-SO3 No communication between charging stations on the WAN: There is no direct communication between charging stations on the WAN interface. The charging stations can only communicate with the CPO central system.	• OR 12 Protecting networks
8.24-SO3 Key and password management process: The charge point operator manages the keys and passwords of the devices so that they are properly	• OR 13 Key and password management process

protected and can be updated when needed.	

4.2 Rationale for the requirements applicable to the CPO central system

Table 8 shows how the requirements in Section 3.1 cover the security objectives that apply to the CPO central system. The coverage is further explained below.

Table 8: Selection of security requirements from IEC 62443-3-3 to meet the security objectives for the CPO central system.

Security Objective	***IEC 62443-3-3 requirements***
8.3 Information access restriction	
8.3-SO1 Least privileges on the WAN interface: The CPO central system enforces access control on the WAN so that users on the interface can only access the functions they need.	• SR 2.1 Authorization enforcement • SR 2.1 RE1 Authorization enforcement for all users (humans, software processes, and devices)
8.3-SO2 Role separation on the market interface: The CPO central system enforces access control on the market interface with separate roles for mobility service providers, roaming platforms, and DSO systems so that they can only access the functions they need for their role.	• SR 2.1 Authorization enforcement • SR 2.1 RE1 Authorization enforcement for all users (humans, software processes, and devices)
8.3-SO3 Centrally managed, role-based access control for customer service representatives, engineers, and server administrators: The CPO central system enforces role-based access control for customer service representatives, engineers, and server administrators with individual user accounts managed on a central server.	• SR 1.3 Account management • SR 1.3 RE1 Unified account management • SR 1.4 Identifier management • SR 2.1 Authorization enforcement • SR 2.1 RE1 Authorization enforcement for all users (humans, software processes, and devices) • SR 2.1 RE2 Permission mapping to roles

8.3-SO4 Restrictions on switching commands: The CPO central system does not allow engineers and customer representatives to switch charging on or off on many charging stations at the same time, for instance by limiting the number of switching commands per user per hour.	• SR 2.1 Authorization enforcement
8.3-SO5 Individual accounts for customers: The CPO central system supports individual accounts for customers and enforces access control so that they can only access the functions they need.	• SR 1.3 Account management • SR 1.4 Identifier management • SR 2.1 Authorization enforcement • SR 2.1 RE1 Authorization enforcement for all users (humans, software processes, and devices)
8.5 Secure authentication	
8.5-SO1 Mutual authentication for the charging stations, mobility service provider, roaming platform, and DSO systems: The CPO central system enforces mutual authentication with the charging stations, mobility service provider, roaming platform, and DSO system. Devices on each side uniquely identify themselves and allow the other side to authenticate them. They only provide access after having authenticated the other side's identity.	• SR 1.2 Software process and device identification and authentication • SR 1.2 RE1 Unique identification and authentication • SR 1.9 Strength of public key authentication • SR 2.6 Remote session termination • SR 4.3 Use of cryptography
8.5-SO2 Authentication with individual passwords for customers, customer service representatives, engineers, and server administrators: The CPO central system enforces mutual authentication for customers, customer representatives, engineers, and server administrators. Representatives, engineers, and administrators use individual credentials. The login procedure is protected against known attacks.	• SR 1.1 Human user identification and authentication • SR 1.1 RE1 Unique identification and authentication • SR 1.5 Authenticator management • SR 1.7 Strength of password-based authentication • SR 1.7 RE1 Password generation and lifetime restriction for human users

	• SR 1.9 Strength of public key authentication • SR 1.10 Authenticator feedback • SR 1.11 Unsuccessful login attempts • SR 2.5 Session lock • SR 2.6 Remote session termination • SR 4.3 Use of cryptography
8.5-SO3 Multifactor authentication for server administrators on server maintenance interface: The CPO central system enforces multifactor authentication for server administrators on the server maintenance interface with a login procedure that is protected against known attacks.	• SR 1.1 RE2 Multifactor authentication for untrusted networks
8.7 Protection against malware	
8.7-SO1 Active malware protection in the CPO central system: Hosts in the CPO central system, are actively protected against malware, for instance through anti-virus software or endpoint protection software.	• SR 3.2 Malicious code protection
8.8 Management of technical vulnerabilities	
8.8-SO1 Hardening over the local maintenance or server maintenance interface: Server administrators can harden hosts in the CPO central system over the server maintenance interface or from engineering workstations. They can disable unneeded functions to reduce the likelihood of vulnerabilities and enable security functions available on the hardware and software platforms to reduce their possible impact.	• SR 3.2 Malicious code protection • SR 7.7 Least functionality

8.9 Configuration management	
8.9-SO1 Managing network and security configurations over the server maintenance interface: The CPO central system allows server administrators to manage and monitor the network and security configurations of the CPO central system from the server maintenance interface. *Remark:* Changes to configurations are logged according to objective 8.15-SO1.	• SR 7.6 Network and security configuration settings
8.10 Information deletion	
8.10-SO1 Personal information deletion: The CPO central system can securely erase sensitive information when no longer required to comply with privacy regulations such as the GDPR.	• SR 4.2 Information persistence
8.11 Data masking	
8.11-SO1 Data masking: The CPO central system has the capability of performing data masking, pseudonymization, or anonymization on the sensitive data stored in the system.	• SR 4.1 Information confidentiality • SR 4.1 RE1 Protection of confidentiality at rest or in transit via untrusted networks
8.13 Information backup	
8.13-SO1: Automated backups for the CPO central system: The CPO central system supports making automated backups of the configurations and data.	• SR 7.3 Control system backup • SR 7.3 RE1 Backup verification • SR 7.3 RE2 Backup automation • SR 7.4 Control system recovery and reconstitution
8.15 Logging	

8.15-SO1 Integration with SIEM system: The servers in the CPO central system log all relevant security events, such as access control events, and changes to the configuration and software. The servers can store the logs locally for forensic analysis. They can send them to a Security Information and Event Management (SIEM) system in a commonly supported format so that they can be analysed to detect incidents.	• SR 2.8 Auditable events • SR 2.8 RE1 Centrally managed, system-wide audit trail • SR 2.9 Audit storage capacity • SR 2.10 Response to audit processing failures • SR 3.9 Protection of audit information • SR 6.1 Audit log accessibility • SR 6.1 RE1 Programmatic access to audit logs
8.17 Clock synchronization	
8.17-SO1 Clock synchronization for the CPO central system: The CPO central system synchronizes time with a central source to have reliable timestamps for security events.	• SR 2.11 Timestamps • SR 2.11 RE1 Internal time synchronization • SR 2.11 RE2 Protection of time source integrity
8.19 Installation of software on operational systems	
8.19-SO1 Software updates over the server maintenance interface: Server administrators can update the software and firmware in the CPO central system over the server management interface or from engineering software. Hosts in the CPO central system check the authenticity of firmware or software before installation through digital signatures.	• SR 1.8 Public key infrastructure certificates • SR 1.9 Strength of public key authentication • SR 3.4 Software and information integrity • SR 4.3 Use of cryptography
8.20 Network security	
8.20-SO1 Cryptographic protection of communication confidentiality and integrity on the WAN, management portal, market interface, and server maintenance interface: The CPO central system protects the integrity and	• SR 1.9 Strength of public key authentication • SR 3.1 Communication integrity • SR 3.1 RE1 Cryptographic integrity protection • SR 3.8 Session integrity

confidentiality of communication on the WAN, management portal, market interface, and server maintenance interface using cryptographic measures. The measures allow to verify the source of messages and protect against replay and man-in-the-middle attacks.	• SR 4.1 Information confidentiality • SR 4.1 RE1 Protection of confidentiality at rest or in transit via untrusted networks • SR 4.1 RE2 Protection of confidentiality across zone boundaries • SR 4.3 Use of cryptography
8.22 Segregation of networks	
8.22-SO1 Logical network segregation on the WAN, management portal, market interface, and server maintenance interface: The CPO central system is segregated from other zones on the WAN, management portal, market interface, and server maintenance interface. Only normal incoming and outgoing connections are allowed through the network perimeter. The communication load can be controlled at the perimeter.	• SR 5.1 Network segmentation • SR 5.2 Zone boundary protection • SR 5.2 RE1 Deny by default, allow by exception • SR 7.1 Denial of service protection • SR 7.1 RE1 Manage communication loads
8.24 Use of cryptography	
8.24-SO1 Key and password management over the server maintenance interface: Server administrators can manage all passwords and keys used on the CPO central system server efficiently over the server maintenance interface.	• SR 1.5 Authenticator management • SR 1.8 Public key infrastructure certificates • SR 1.9 Strength of public key authentication • SR 4.3 Use of cryptography

4.3 Rationale for the charging stations and charging plazas

Table 9 shows how the requirements in Section 3.3 cover the security objectives that apply to charging stations and charging plazas. The coverage is further explained below. Note that the physical security requirements to the CPO central system are covered by the process requirements, as there are no related requirements in IEC 62443-3-3.

Table 9: Selection of security requirements from IEC 62443-3-3 to meet the security objectives for the charging station. Additional requirements not in IEC 62443-3-3 are given in italics.

Objective	***IEC 62443-3-3 requirements***
8.3 Information access restriction	
8.3-SO6 Least privileges on the WAN, authentication terminal, electric vehicle, local maintenance, LAN, and EMS interfaces: The charging station or plaza enforces access control on the WAN, authentication terminal, electric vehicle, local maintenance, LAN, and EMS interfaces so that user group with access to the interface can only access the functions they need.	• SR 2.1 Authorization enforcement • SR 2.1 RE1 Authorization enforcement for all users (humans, software processes, and devices)
8.5 Secure authentication	
8.5-SO4 Role-based authentication for engineers: Engineers identify to the charging station with information that allows the zone to determine its role. The zone authenticates the user's role and assigns them access rights based on the role.	• SR 1.1 Human user identification and authentication • SR 1.2 Software process and device identification and authentication • SR 1.7 Strength of password-based authentication • SR 1.9 Strength of public key authentication • SR 2.6 Remote session termination • SR 4.3 Use of cryptography
8.5-S05 Unique authentication for the CSMS and electric vehicles: The CSMS and electric vehicles uniquely identify themselves to the zone. The zone authenticates their identity and assigns them access rights based on their role.	• device identification and authentication • SR 1.9 Strength of public key authentication • SR 2.6 Remote session termination • SR 4.3 Use of cryptography

8.5-SO6 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.	• SR 1.1 Human user identification and authentication
8.8 Management of technical vulnerabilities	
8.8-SO2 Hardened by default: The charging stations and charging plaza devices 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.	• SR 3.2 Malicious code protection • SR 3.5 Input validation • SR 7.7 Least functionality
8.9 Configuration management	
8.9-SO2 Automated configuration management: The charging station can be restored from a backed-up configuration automatically by the CPO central system.	• SR 7.3 Control system backup • SR 7.3 RE1 Backup verification • SR 7.3 RE2 Backup automation • SR 7.4 Control system recovery and reconstitution
8.9-SO3 Secure configuration by default: The charging stations and charging plaza devices are 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.	• SR 1.5 Authenticator management • SR 7.6 Network and configuration settings

8.10 Information deletion	
8.10-SO2 Personal information deletion: The charging station can securely erase sensitive information when no longer required to comply with privacy regulations such as the GDPR.	• SR 4.2 Information persistence
8.15 Logging	
8.15-SO2 Collecting security events from the charging station 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. *Remark:* The CPO central system can then forward the security logs to a SIEM system according to 8.15-SO1.	• SR 2.8 Auditable events • SR 2.9 Audit storage capacity • SR 2.10 Response to audit processing failures • SR 3.9 Protection of audit information • SR 6.1 Audit log accessibility • SR 6.1 RE1 Programmatic access to audit logs
8.17 Clock synchronization	
8.17-SO2 Clock synchronization for the charging station: The charging station or plaza synchronizes time with a central source to have reliable timestamps for security events.	• SR 2.11 Timestamps • SR 2.11 RE1 Internal time synchronization • SR 2.11 RE2 Protection of time source integrity
8.19 Installation of software on operational systems	
8.19-SO2 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 can check the authenticity of firmware through digital signatures.	• SR 1.8 Public key infrastructure certificates • SR 1.9 Strength of public key-based authentication • SR 3.4 Software and information integrity • SR 4.3 Use of cryptography

8.20 Network security	
8.20-SO2 Cryptographic protection of communication confidentiality and integrity on the WAN interface: The charging station protects the integrity and confidentiality of communication on the WAN interfaces using cryptographic measures. The measures allow to verify the source of messages and protect against replay and man-in-the-middle attacks.	• SR 1.9 Strength of public key-based authentication • SR 3.1 Communication integrity • SR 3.1 RE1 Cryptographic integrity protection • SR 3.8 Session integrity • SR 4.1 Information confidentiality • SR 4.1 RE1 Protection of confidentiality at rest or in transit via untrusted networks • SR 4.1 RE2 Protection of confidentiality across zone boundaries • SR 4.3 Use of cryptography
8.20-SO3 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	• SR 3.5 Input validation • SR 7.1 Denial-of-service protection
8.22 Segregation of networks	
8.22-SO2 Logical network segregation on the charging station WAN: The charging station is segregated from other zones on the WAN interface. Only normal incoming and outgoing connections are allowed through the network perimeter. The communication load can be controlled at the perimeter.	• SR 5.1 Network segmentation • SR 5.2 Zone boundary protection • SR 5.2 RE1 Deny by default, allow by exception • SR 7.1 Denial-of-service protection • SR 7.1 RE1 Manage communication loads
8.24 Use of cryptography	
8.24-SO2 Automated key and password management over the WAN: All passwords	• SR 1.5 Authenticator management

and keys used in the charging station can be updated automatically through remote access from the CPO central system.	• SR 1.8 Public key infrastructure certificates • SR 1.9 Strength of public key-based authentication • SR 4.3 Use of cryptography

References

[1] ISA/IEC, "IEC 62443-3-3: Security for industrial automation and control systems - Part 3-3: System security requirements and security levels".

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

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

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

[5] ENCS, EV-311-2022: IEC 62443 requirements for EV charging stations, 2022.

[6] ENCS, "EV-312: Implementing IEC 62443-4-2 requirements in OCPP 2.0.1," 2025.

[7] ENCS, "EV-313: Coverage of EN 18031 requirements by the IEC 62443 requirements for EV charging stations," 2025.

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

[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 electricle vehicle for control of d.c. charging in the Combined Charging System," 2014.

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

[14] IEC/ISA, IEC 62443-2-4: Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers, 2017.

[15] NIST, "NIST Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management," 2017.

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

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

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