OCPP

IEC 63584

OCPP Security Operations Guide

v2.0, September 2026

Table of Contents

Version History

Version	Date	Description
1.0	January 2026	First release version
2.0	September 2026	Second release version

Acknowledgements

The Open Charge Alliance would like to thank the people that contributed to the contents of this Security Operations Guide. Besides the members of the Cyber Security Taskgroup, we would like to give a special thanks to the following people for their valuable research / input for this publication:

- Mohammad Ali Sayed (Independent Researcher)
- Wilco van Beijnum (ElaadNL)
- Matthew Jablonski (Assistant Professor, George Mason University)
- Khaled Sarieddine (Independent Researcher)
- Jad Zarzour (Researcher, George Mason University)

1. Introduction

1.1. General introduction

Charging infrastructure is considered critical infrastructure and security issues / breaches can have far-reaching consequences for the electricity grid and society. The OCPP specification therefore has included security as a part of OCPP 2.x and also backported the security to OCPP 1.6 using the OCPP Security Whitepaper (officially titled: "*Improved security for OCPP 1.6-J*"). However, providing security requirements and recommendations in the OCPP specification alone has proven not to be sufficient for vendors to implement secure solutions. Therefore, this Operations Guide provides guidance to implementers of OCPP Charging Stations and CSMSs, to build more secure solutions, keeping in mind interoperability. This guidance provides recommendations that can also be found in the OCPP specification *and* additional guidance to use OCPP features in a secure way. To make clear what is already in the specification and what is not, sections / text blocks are marked as:

- *"About the OCPP specification"* - this means that this is already described in the OCPP specification.
- *"Upcoming OCPP specification updates (errata & additions)"* - this indicated that this is expected to be added to the next OCPP version (and are already possible in the current OCPP 2.x versions as extensions).
- *"OCA recommendations beyond OCPP"* - this concerns recommendations that are out of scope of OCPP, but are needed for a security implementation of OCPP in a Charging Station or CSMS.

Security is becoming part of more and more regulations. For this reason, the next chapter Regulations vs measures discusses a number of regulations that have been analyzed. An overview is provided on what security measures must be taken for each of these regulations.

NOTE	This Security Operations Guide refers to requirements from the OCPP specification. In case of a conflict in the numbered requirements referenced in this document and the main OCPP 2.x specification, the OCPP 2.x specification is leading.

NOTE	This guide is provided for informational purposes only and is intended to assist implementers in understanding security guidelines, considerations and applicable regulations. While every effort has been made to ensure the accuracy and completeness of the information, the Open Charge Alliance (OCA) does not warrant that the guide is free from errors, omissions, or misinterpretations. Implementers are solely responsible for assessing the applicability of the information to their specific products, services, and jurisdictions, and for ensuring compliance with all applicable laws, regulations, and contractual requirements.

1.2. What's new in this version?

Version 2 of the Security Operations Guide introduces several updates and extensions to improve the applicability of the guide and provide more detailed security guidance for stakeholders across the EV charging ecosystem. The main changes compared to the previous version are:

- **Introduction of numbered requirements**
  Security recommendations have been converted into numbered requirements to improve traceability and referencing.
- **Separation of CSMS and CPO responsibilities**
  The previous CSMS-focused requirements have been reorganized into separate sections for CSMS providers and Charge Point Operators (CPOs).
- **Extended CSMS and CPO security requirements**
  The requirements for CSMS providers and CPOs operating these systems, have been expanded to provide more guidance on security operations, including additional measures to support secure deployment and operation of charging infrastructure.
- **Introduction of a Post-Quantum Security Policy**
  A new Security Policy for Post-Quantum Cryptography has been added to prepare for the transition towards post-quantum cryptography.
- **Introduction of JC-STAR considerations**
  The guide now includes references to the JC-STAR Level 1 cybersecurity certification scheme.
- **Addition of a Defense-in-Depth approach**
  A new section on defense in depth has been introduced, which includes complementary security controls that can be applied to OCPP implementations.
- **Guidance on Local Controllers**
  A new section has been added to address security considerations for Local Controllers.

2. Regulations vs. security measures

2.1. Introduction to regulations

The European Union is setting more strict regulations for cybersecurity. Charging Station manufacturers already need to comply with the Radio Equipment Directive (RED) cybersecurity requirements and will soon need to meet the requirements in the Cyber Resilience Act (CRA) and Measuring Instruments Directive (MID) if they want to sell Charging Stations in the EU. Charge Point Operators in the EU will be seen as critical infrastructure and will have to meet the NIS2 and NCCS requirements. The corresponding North American regulations are still less strict, but do include some relevant requirements. For instance, the Cybersecurity Information Sharing Act which facilitates information sharing between government and private sector but is not setting technical controls. In Canada, the Canadian Cyber Security Strategy and Critical Infrastructure Protection (CIP) programs aim to improve cybersecurity for critical sectors but lack a unified directive like NIS2.
However, in the United States, several states have their own cybersecurity laws. The California Consumer Privacy Act (CCPA) is one of them and is of relevance for Charging Stations implementing OCPP.

In this chapter the relevant security regulations are shortly discussed and the relation to the security requirements and recommendations from this whitepaper is presented. The security regulations that have been analyzed for coverage by OCPP are the following:

Regulation	Region	Year	Reference to original regulation
Radio Equipment Directive (RED)	EU	2024	[EN_18031-1], [EN_18031-2] and [EN_18031-3]
Cyber Resilience Act (CRA)	EU	2024	[CRA]
Measuring Instruments Directive (MID)	EU	2014/2024 / 2026	[MID-1], [MID-2] and [MID-3]
Network and Information Systems Directive 2 (NIS2)	EU	2022	[NIS-2]
Network Code on Cybersecurity (NCCS)	EU	2024	[NCCS]
Cybersecurity Maturity Model Certification (CMMC)	US	2025	[CMMC]
California Consumer Privacy Act (CCPA)	US	2024	[CCPA]
The NIST Handbook 44	US	2025	[NIST]
Japan Cyber-Security Technical Assessment Requirements (JC-STAR)	Japan	2024	[STAR-1]

In the following sections, each regulation is shortly introduced. After the introduction of the regulations, an overview of the regulations vs the security requirements and recommendations described in this Operations Guide is given. Vendors that need to adhere to a regulation can use this as a checklist to make their OCPP implementation comply to a regulation.

2.1.1. Radio Equipment Directive (RED)

The Radio Equipment Directive (2014/53/EU), published by DG GROW in 2014, ensures that devices using radio communication meet cybersecurity requirements before being placed on the EU market. It was passed in 2014 to harmonize the requirements for radio equipment in the EU. In 2021, the European Commission extended the directive with new cybersecurity requirements, and from August 2025 these requirements became mandatory for all internet-connected radio equipment, including Charging Stations.
The RED sets essential requirements for when radio equipment can be sold on the European internal market. These requirements include three points that can be related to cybersecurity in Article 3(3):

- (d) radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;
- (e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;
- (f) radio equipment supports certain features ensuring protection from fraud;

These requirements only apply to classes of products after the Commission adopts a delegated act to supplement the RED. In 2021, the Commission passed a delegated act that made these three points applicable *"to any radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment ('internet-connected radio equipment')"* with the restriction that point (e) only applies if the equipment processes personal data as defined in the GDPR, and point (f) only applies if the equipment allows the user to transfer money, monetary value or virtual currency. The requirements apply from 1 August 2025.

Manufacturers need to determine if their Charging Stations fit the criteria in the delegate act. Note that a device is considered internet-connected if it can communicate over the internet, even when it does not communicate over the internet in normal use. So, even Charging Stations that would normally be used on segregated telecom networks would be considered internet-connected if they can be used with a public SIM card. Many Charging Stations could also be considered to process personal data in the form or UUID and transaction data. At the time of writing this Operations Guide, it is not entirely clear if Charging Stations are considered to transfer money or monetary value, but they are involved in financial transaction. So, interpretations could be possible in which all three points (d), (e), and (f) would apply to Charging Stations.

Manufacturers need to demonstrate compliance with the RED through a conformity assessment. There are different conformity assessment modules allowed. Module A, internal production control, is easiest to apply, as manufacturers may do a self-assessment. Using one of the other options (module B+C or module H) would require independent tests and audits. There is limited capacity available for these since all radio equipment will need to go through the conformity assessment by 1 August 2025. Manufacturers may, however, only use module A if they follow a harmonized standard[1]. A harmonized standard for cybersecurity was adopted by the Commission on 28 January 2025. The standard, EN 18031, consists of three parts:

- **EN 18031-1** covers point (d) and applies to all internet-connected radio equipment.

- **EN 18031-2** covers point (e) applies to internet-connected radio equipment processing personal data.
- **EN 18031-3** covers point (f) and applies to internet-connected radio equipment that allows users to transfer money, monetary value, or virtual currency.

The standards mostly contain requirements comparable to those in the ENCS requirements ENCS Security Requirements that Charging Stations must meet, such as not allowing Security Profile 1 on unsecured networks. Please refer to Regulations vs. security measures for an overview of the security requirements from the three standards that are relevant for CSMSs and Charging Stations.

The European Commission has stated that the RED delegated act will be repealed once the CRA becomes applicable on 11 December 2027. The Commission has published a draft act repealing the delegated act.

2.1.2. Cyber Resilience Act (CRA)

The Cyber Resilience Act (2024/2847) was proposed by DG CONNECT to establish mandatory cybersecurity requirements for all products with digital elements. It came into force in the EU on December 10, 2024. As of December 11, 2027, manufacturers may only sell products in the EU if they meet these requirements.

Scope

The Cyber Resilience Act covers all products with digital elements, defined as *"software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately."* The CRA would hence apply to Charging Stations but also the CSMS software if it is sold as a product.

A remote data processing solution (RDPS) is defined as *"data processing at a distance for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions."* In most cases, the CSMS would not be considered an RDPS, as it is not developed under the responsibility of the manufacturer. But systems developed by the manufacturer to configure Charging Stations or perform firmware updates could be considered RDPS.

The exact rules for when a remote system is an RDPS are not clear yet. The European Commission has provided guidance, which was published on 27 July 2026 ([CRA-GD]). The guidance gives three main criteria for being an RDPS:

1. whether data processing is 'at a distance'
2. whether the absence of such data processing would prevent the product from performing one of its functions
3. whether the software is designed and developed by the manufacturer, or under its responsibility.

Manufacturers should try to apply these criteria, but this will not always be easy in practice.

Essential cybersecurity requirements

According to the CRA, all products with digital elements will need to meet certain essential cybersecurity requirements listed in CRA Annex I of the CRA. These are high level requirements stated in legal language.

They are divided into two types:

1. *Cybersecurity requirements relating to the properties of products with digital elements* covering the technical properties of the products. Manufacturers only have to apply them where applicable and based on a risk assessment they perform.
2. *Vulnerability handling requirements* covering the vulnerability handling process at the manufacturer. Manufacturers must handle vulnerabilities effectively for the support period of the product (which is at least 5 years).

Conformity assessments

While the CRA and RED have similar conformity assessment modules, the rules for which modules manufacturers may use are different. Under the CRA, the available modules depend on the categorization of products. If a product is classified as important or critical, only the stricter conformity assessment modules may be used, see table below:

Table 1. Conformity assessments modules allowed by the CRA for different categories of products.

Assessment module: **Product category:**	**A: Internal control**	**B: EU Type examination** **C: Internal production control**	**H: Full Quality Control**	**Certification**
Default	Allowed	Allowed	Allowed	Allowed
Important - class 1	Allowed if a harmonized standard is available.	Allowed	Allowed	Allowed
Important - class 2	Not allowed	Allowed	Allowed	Allowed
Critical	Not allowed	Allowed unless certification is required by a delegated act.		Allowed

The CRA contains lists of important and critical product categories in CRA Annexes III and IV. The Commission has published a delegated act giving technical descriptions of these products (see [CRACAT]).

Manufacturers need to determine if their Charging Stations fall under an "important" or "critical" product category. If a Charging Station implements tamper detection, manufacturers should analyze if it falls under the critical category of hardware devices with security boxes, described as:

"Hardware products with digital elements that incorporate a hardware physical envelope providing countermeasures against physical attacks, including tamper evidence, resistance or response, and that are

designed to securely store, process, and manage sensitive data and cryptographic operations. This category includes but is not limited to payment terminals, hardware security modules, and tachographs that meet the above definition."

If a Charging Station is categorized as critical, the manufacturer needs to show compliance through module B (EU-type examination) or module H (Conformity based on full quality assurance). Under module B, the manufacturer sends the Charging Station to a notified body (i.e., a government appointed test lab for the CRA) to undergo testing against the CRA requirements. Under module H, the manufacturer sets up a quality system that ensures that products are designed, developed and produced according to the CRA requirements. The notified body then assesses the quality management system.

If a manufacturer determines that a Charging Station is not important or critical, Charging Stations would fall into the default category and manufacturers can use internal control for the conformity assessment. The manufacturer is then solely responsible for complying with the CRA essential requirements mentioned above. There are no tests or audits by an independent notified body.

CRA standards

The Commission has asked European Standardization Organizations to develop standards for the CRA that turn the high-level essential cybersecurity requirements into detailed technical specifications. Manufacturers can also choose to follow these standards to be sure that they correctly interpret the CRA essential requirements.

The standards are expected to become available in 2026 and 2027. For Charging Stations the standards in Table 2 would be applicable. At the time of writing these standards are still under development. So, the analysis below is based on the available drafts.

Table 2. CRA standards applicable to Charging Stations

Essential requirements from CRA Annex I	Standards	Planned publication date
Part I (1)	EN 40000-1-2 Cybersecurity requirements for products with digital elements — Principles for cyber resilience	2026/08/30
Part I (2)	EN 40000-1-4 Cybersecurity requirements for products with digital elements – Generic Security Requirements	2027/10/30
	EN IEC 62443-4-2:2019/prAA: Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components	2026/10/30
Part II	EN 40000-1-3 Cybersecurity requirements for products with digital elements – Vulnerability Handling	2026/08/30

The EN 40000-1-2 standard includes principles for designing, developing and producing products to ensure an appropriate level of cybersecurity. It describes cybersecurity risk management activities to cover the CRA requirements for manufacturer risk assessments. In addition, it covers product cybersecurity lifecycle activities including developing product cybersecurity requirements, implementing them, and verifying and validating them. The lifecycle activities also cover secure production, distribution and decommissioning.

For implementing the product property requirements in CRA Annex I Part I (2), there are two options:

1. *The horizontal standard EN 40000-1-4*. This standard has been developed to be applicable to all types of digital products. It is derived from the EN 18031 standard that was developed for the Radio Equipment Directive delegated act on cybersecurity (which will be replaced by the CRA when the CRA goes into force).
2. *The industrial standard EN IEC 62443-4-2*. This standard is a development of the IEC 62443-4-2 standard that was specifically developed for industrial products such as embedded devices. CEN/CLC is updating the standard so that manufacturers can use it to conform to the CRA.

The IEC 62443-4-2 standard, is also the basis for the ElaadNL / ENCS cybersecurity requirements for EV Charging Stations, so that manufacturers can use the ElaadNL / ENCS document to select the applicable requirements from EN IEC 62443-4-2. The document contains a threat analysis which manufacturers could use as input for their CRA risk assessment.

The EN 40000-1-3 defines a vulnerability handling process according to the requirements in CRA Annex I Part II. The process covers receiving, handling, verifying and remediating vulnerabilities, and releasing the remediation to customers.

EN 40000-1-3 is the only standard in Table 2 that is expected to grant "presumption of conformity". This means that the European Commission will cite the standard as a harmonized standard. Manufacturers implementing the standard then automatically comply with the relevant parts of the CRA essential requirements. The other standards only provide guidance and do not guarantee compliance.

Reporting obligations

Besides implementing the essential cybersecurity requirements, manufacturers must also report any actively exploited vulnerabilities in their product and severe incidents having an impact on the security of the product to their national Computer Security Incident Response Team (CSIRT) and to ENISA. ENISA is developing a reporting platform for this purpose. Vulnerabilities must already be reported as of September 11th 2026.

2.1.3. Measuring Instruments Directive (MID)

The Measuring Instruments Directive (2014/32/EU), developed by DG GROW and applicable since 20 April 2016, harmonizes EU rules for making measuring instruments available on the market. Directive (EU) 2026/706, adopted on 11 March 2026 and entering into force on 9 April 2026, amends the MID by introducing requirements for measuring systems used for electric vehicle supply equipment.

The MID contains some requirements related to cybersecurity under the essential requirements in Annex I

8. Protection against corruption
8.1. The metrological characteristics of a measuring instrument shall not be influenced in any inadmissible way by the connection to it of another device, by any feature of the connected device itself or by any remote

device that communicates with the measuring instrument.
8.2. A hardware component that is critical for metrological characteristics shall be designed so that it can be secured. Security measures foreseen shall provide for evidence of an intervention.
8.3. Software that is critical for metrological characteristics shall be identified as such and shall be secured. Software identification shall be easily provided by the measuring instrument. Evidence of an intervention shall be available for a reasonable period of time.
8.4. Measurement data, software that is critical for measurement characteristics and metrologically important parameters stored or transmitted shall be adequately protected against accidental or intentional corruption.
8.5. For utility measuring instruments the display of the total quantity supplied or the displays from which the total quantity supplied can be derived, whole or partial reference to which is the basis for payment, shall not be able to be reset during use.

Manufacturers can show conformity with the MID by implementing so-called normative documents, similar to the harmonized standards for the RED and CRA. Normative documents for the MID are developed by the International Organization of Legal Metrology (OIML).[2] The OIML developed in 2022 the guide OIML G 22 for Electric Vehicle Supply Equipment (EVSE). This is not yet a normative document for the MID, as it would first have to be adopted by the European Commission. But the structure and scope suggest it was developed with future MID adoption in mind.

Please note that as the detailed implementation guidance is expected to be provided through the relevant WELMEC Guide, this section will be updated in the next version of this guide.

2.1.4. Network and Information Systems Directive 2 (NIS2)

The NIS2 Directive (EU 2022/2555), coordinated by DG CONNECT was published in December 2022 and member states are currently transposing it into national law. It aims to strengthen cybersecurity across the EU by introducing more stringent requirements for a broader range of sectors. The European Commission passed the NIS2 directive as the successor to the NIS directive from 2016.

Charge Point Operators are covered by the NIS2 directive as operators of recharging points, and they do fall under the electricity subsector. So, the risks they create to the electricity sector will be regulated.
The NIS2 directive uses thresholds on the size of entities to determine if they are in scope. All CPOs that are medium-sized or larger (as defined in the Annex to Recommendation 2003/361/EC [ENT-SIZES]) are in scope of the NIS2 directive. If they are medium-sized they are considered important entities. If they are larger, they are considered essential entities.
Regarding other parties that fall within the scope of NIS2:

- Charging Station manufacturers are considered *important* entities under the categories “Manufacture of computer, electronic and optical products” and “Manufacture of electrical equipment.”
- Electric vehicle manufacturers are considered *important* entities under the category “Manufacture of motor vehicles, trailers and semi-trailers.”
- Cloud service providers are considered *essential* entities under the category “Cloud service providers.”

- Charging Station installers are possibly considered *essential* entities under the category "Managed service providers."

As with CPOs, size-based thresholds apply to all these parties.

The NIS2 directive requires CPOs to take appropriate and proportionate measures to manage cybersecurity risks. It leaves relatively open what these measures should be. Only a very high-level list of topics to be covered is included in Article 21(2).

Many member states are however developing their own sets of mandatory measures that are much more detailed. Examples of measures developed by different member states for the original NIS:

- Spanish National Security Scheme (see [SNSS])
- Italian Security Measures in Annex B of DCPM 81/2021 (see [DCPM])
- French security rules (see [FSR])

These rules are however now being updated because of the introduction of the NIS2 directive. CPOs should monitor the controls for the countries in which they are active. It is difficult to extract general technical measures for the OCPP operational security guidelines at this point. Besides taking risk management measures, CPOs will also have to report cybersecurity incidents. The reporting thresholds are defined by each EU member state.

2.1.5. Network Code on Cybersecurity (NCCS)

The Network Code on Cybersecurity (EU 2024/1366) is a sector-specific cybersecurity regulation. It is a delegated act developed by DG ENER and published in March 2024. It aims to create a European baseline for the cybersecurity of cross-border electricity flows. CPOs are in scope of the NCCS, but they only need to apply their measures if they are large enough to cause cross-border disruptions to the electricity sector. As the European electricity system is connected, a cyber-attack in one member state could cause problems in the electricity system of another. The NCCS should manage these risks in a coordinated way and enforce a harmonized level of cybersecurity.

Whether a CPO is large enough to cause cross-border disruptions to the electricity sector - and is thus in scope - is determined through so-called high- and critical-impact thresholds. A provisional list of thresholds has been published by ENTSO-E (see [ENTSO-E]). The thresholds differ per member country, the lowest "high-impact" thresholds that apply in some member countries are 250 MW of total charging capacity of all charging points operated by the CPO.
As for the NIS2 directive, the NCCS will require CPOs to take measures to manage cybersecurity risks. The measures are more detailed at a European level to create a harmonized security baseline. They include:

- Setting up a cybersecurity management system for instance based on ISO/IEC 27001
- Performing structured risk assessments taking into account the possible impact on the electricity system
- Implementing minimum and advanced cybersecurity controls selected based on a regional cybersecurity risk assessment

- Implementing supply chain security controls to ensure secure procurement of new components and systems, such as Charging Stations

The measures will not include detailed technical requirements. Procurement recommendations could be developed to help entities meet the supply chain controls. These could include recommendations on using technical requirements during procurement. But the recommendations are not binding.

CPOs will also need to report cybersecurity incidents that may cause disruptions to the electricity system. Exact thresholds for reporting still need to be defined.

2.1.6. ENCS Security Requirements

ElaadNL - the Dutch knowledge and innovation center for smart charging infrastructure - and ENCS[3] - the European Network for Cyber Security, a non-profit organization with the mission to improve cyber security by sharing knowledge - have developed a set of security requirements for charging infrastructure. The two main documents are:

- EV-211: Security requirements from IEC 62443 for EV charging infrastructure. Local governments can use these requirements when procuring public Charging Stations from a Charge Point Operator. (see [EV-211] for details and link to document)
- EV-311 Security requirements from IEC 62443 for procuring EV Charging Stations. CPOs and others can use these requirements when procuring Charging Stations from a manufacturer. (see [EV-311] for details and link to document)

The requirements are based on the IEC 62443 standard for industrial cybersecurity. Requirements have been selected from this standard based on a threat analysis.

Supporting documents are available explaining how the ElaadNL and ENCS requirements compare to the requirements in the EN 18031 harmonized standard for the Radio Equipment Directive, and how the requirements can be implemented in OCPP. See [EV-312] and [EV-313] for details and link to document. The documents are informative and included in the basic set recommended for public Charging Stations by NKL, the Dutch national knowledge platform for charging infrastructure that works with policymakers, knowledge institutions, grid operators and market parties. Some cities and provinces include them in their tender requirements.

2.1.7. Cybersecurity Maturity Model Certification (CMMC)

The CMMC [4] was originally developed in January 2020 by the U.S. Department of Defense (DoD) to ensure that contractors and suppliers implement adequate cybersecurity protections for Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). It provides a standardized framework for assessing and strengthening the cybersecurity of suppliers. The CMMC is relevant only if a federal agency buys EV Charging Stations directly or when used in defense-related contracts. However, given the cybersecurity prescriptions, it is still a certification noteworthy for OCPP users. In version 2.0 of CMMC, Charging Stations fit in the ‘specialized assets’ category in the CMMC (devices that can’t be fully secured but still process/store data, including IoT/IIoT, OT). The CMMC follows a tiered model, which includes three maturity levels:

- Level 1: Basic cyber hygiene - aligns with 15 practices from FAR 52.204-21.
- Level 2: Advanced cyber hygiene - aligned with NIST SP 800-171 R2 (110 practices).
- Level 3: Expert level - 134 requirements (110 based on NIST SP 800-171 R2 + 24 based on NIST SP 800-172 (select requirements, more advanced)).

Assessments are required as well to verify the implementation of the requirements.

2.1.8. The NIST Handbook 44

The NIST Handbook 44, published and maintained annually by the National Institute of Standards and Technology (NIST), sets technical requirements and tolerances for weighing and measuring devices, including electric vehicle (EV) Charging Stations. Similarly to the Measuring Instruments Directive (MID) in the European context, the NIST Handbook 44 [5] gives general requirements for measuring instruments used in the U.S. Section 3.40 “Electric Vehicle Fueling Systems” was added to NIST Handbook 44 as a tentative code in 2015. Later, in July 2022, its status was changed from “tentative” to “permanent”, with the change becoming effective on January 1, 2023. This section establishes requirements for EV Charging Stations when the sale of electricity is based on metered kilowatt-hours. Handbook 44 is published annually by NIST but becomes legally binding through adoption by the National Conference on Weights and Measures (NCWM). Most U.S. states adopt Handbook 44 by reference into their weights and measures laws.

The Handbook 44 contains some requirements related to cybersecurity:

- *S.3.1. Metrological Components. – An EVSE measuring system shall be designed and constructed so that metrological components are adequately protected from environmental conditions likely to be detrimental to accuracy. The system shall be designed to prevent undetected access to adjustment mechanisms and terminal blocks by providing for application of a physical security seal or an audit trail.*
- *S.3.3. Provision for Sealing. – For devices and systems in which the configuration or calibration parameters can be changed by use of a removable digital storage device, security shall be provided for those parameters as specified in G-S.8.2. Devices and Systems Adjusted Using Removable Digital Storage Devices. For parameters adjusted using other means, the following applies. Adequate provision shall be made for an approved means of security (e.g., data change audit trail) or physically applying security seals in such a manner that no adjustment can be made of:*

(a) each individual measurement element;
(b) any adjustable element for controlling voltage or current when such control tends to affect the accuracy of deliveries;
(c) any adjustment mechanism that corrects or compensates for energy loss between the system and vehicle connection; and
(d) any metrological parameter that detrimentally affects the metrological integrity of the EVSE or system. When applicable, the adjusting mechanism shall be readily accessible for purposes of affixing a security seal. Audit trails shall use the format set forth in Table S.3.3. Categories of Device and Methods of Sealing. (Amended 2019)

- *S.4.1. Diversion of Measured Electricity. – No means shall be provided by which any measured* *electricity can be diverted from the measuring device. S.4.1.1. Unauthorized Disconnection. – Means shall be provided to automatically terminate the transaction in the event that there is an unauthorized break in the connection with the vehicle.*

2.1.9. California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) was developed by the California Legislature and signed into law in 2018. The CCPA imposes cybersecurity-related duties on businesses that process California residents' personal data. For OCPP deployments, these duties primarily concern reasonable security practices, encryption of data, protection of sensitive personal information, and incident handling.

After California passed the CCPA in 2018, other states began drafting and enacting their own consumer privacy laws that reflect or build upon elements of the CCPA and go beyond breach notification statutes. For example, states like Virginia (VCDPA), Colorado (CPA), Connecticut (CDPA) and others have followed CCPA's lead in passing their own comprehensive privacy acts. The other acts, however, require controllers to implement appropriate technical and organizational measures to protect data, but liability for unencrypted breaches like in CCPA is unique.

2.1.10. Japan Cyber-Security Technical Assessment Requirements (JC-STAR)

The Japan Cyber-Security Technical Assessment Requirements (JC-STAR) is a Japanese initiative designed to confirm and visualize the cybersecurity conformance of IoT products. The scheme establishes a framework for assessing the security posture of IoT devices, in harmony with internationally recognized standards such as ETSI EN 303 645 and NISTIR 8425. Participation in JC-STAR is voluntary. JC-STAR defines four levels of security requirements:

- STAR-1 and STAR-2 are based on self-declaration by manufacturers, allowing products to demonstrate conformity.
- STAR-3 and STAR-4 target products intended for government agencies, critical infrastructure, and other high-security environments. These levels require evaluation by the Information-technology Promotion Agency (IPA), Japan, based on reports from independent third-party assessment bodies.

The scheme applies to IoT products capable of sending and receiving data using the Internet Protocol (IP), even if not directly connected to the Internet. The STAR-1 requirements were published in December 2024 (JST-CR-01-01-2024R1[6]), with applications opening on March 25, 2025. Development of STAR-2 requirements is ongoing, while STAR-3 and STAR-4 conformance criteria have not yet been finalized.

To our knowledge, at the time of publication of this guide no decision has been made which JC-STAR level will apply to EV charging infrastructure.

2.1.11. Conclusion

In different regions of the world, various regulation covering information security is in place. Since OCPP is used globally, the Open Charge Alliance aims to distill the impact of all of these regulations and aims to adhere to all. Should you be aware of additional legislation, please contact the Open Charge Alliance at info@openchargealliance.org.

2.2. Regulations vs. security measures

The table below provides an overview of the regulations and the security requirements and recommendations described in this Operations Guide. For each of the security measures / recommendations from the second column it is indicated whether this security measure is required for a regulation.

'R' - security measure is required for a regulation
'R&C' - security measure is required for a regulation and can be demonstrated via certification (see Demonstrating implementation of security requirements).

The sections explain in detail what the measure entails and any specific details per regulation where applicable. A lot of security requirements that are needed for these regulations are an integral part of OCPP and covered by the OCPP Certification program.

Classification	**Security Measure**	**CRA****	**RED directive**			**MID**	**NIS2 / NCCS***	**ENCS**	**CMMC**	**NIST Hb 44**	**CCPA**	**JC-STAR**			
			EN 18031-1	EN 18031-2	EN 18031-3							1	2 (not yet published)	3 (not yet published)	4 (not yet published)
OCPP specification	Implement OCPP security requirements (from OCPP 2.x Core or OCPP 1.6 Core)	R&C	R&C	R&C	R&C	R&C	R&C	R&C	R&C	R&C	R&C				
OCPP specification	Not allowing Security Profile 1 over unsecured networks (see 4.2 and 6.1.2)	R	R	R	R	R	R	R	R		R	R			
OCPP specification / Upcoming OCPP specification updates	Secure firmware updates (see 3.4, 4.8 and 6.1.4)	R	R	R	R			R				R			

Partly OCPP / Partly Beyond OCPP	Use unique credentials during manufacturing (see 4.6)	R	R	R	R			R				R			
Beyond OCPP	Secure storage mechanisms (see 4.9)		R	R	R			R	R			R			
Beyond OCPP	Local security log (see 4.10)	R		R	R			R							
Beyond OCPP	Vulnerability handling (see 4.11 and 5.6)	R	R	R	R			R				R			
Beyond OCPP	Hardening Charging Stations (see 4.12)	R	R	R	R	R		R							
Beyond OCPP	Risk Assessment (see 4.1 and 5.1)	R					R	R	R						
Beyond OCPP	Information sharing and incident reporting (see 5.5.5)						R	R	R						
Beyond OCPP	Information security management system (see 5.2)						R&C	R							
Beyond OCPP	Supply chain security controls (see 5.3)						R	R	R						
Beyond OCPP	Access control for local maintenance (see 4.13)	R	R	R	R			R				R			
Beyond OCPP	Security testing (see 3.7)	R	R	R	R			R	R						
Beyond OCPP	Network resilience (see 4.14)	R	R					R							
Beyond OCPP	Storing passwords (see 4.4.1 and 5.8)	R	R	R	R			R	R			R			
OCPP specification	Preinstalled well-known root CA certificates (see 4.7)							R							
Beyond OCPP	Backups and recovery (see 4.15)	R						R	R						

OCPP specification	Use of FIPS-validated cryptography (see 3.3.2)								R						
Beyond OCPP	Storing personal information (see 4.4.2)			R				R			R	R			
Beyond OCPP	Log monitoring (see 5.5)								R						
Beyond OCPP	Secure storage (see 6.2.4)										R				

* NIS2 and NCCS have a large overlap and are therefore listed in the same column. Note however that they have different thresholds for which CPOs are in scope.

** Under the CRA manufacturers should apply the measures based on a risk assessment. Details on how they should be implemented will be provided in standards that are still under development.

2.3. Demonstrating implementation of security requirements

The measures in the table from 2.2 can partially be demonstrated via certification:

- Following the security requirements of OCPP can be demonstrated via the OCPP Certification Program.
- Setting up a cybersecurity management system can be verified by certifying against ISO/IEC 27001.

For the other requirements that are discussed in this document, no standardized formal verification / certification is available yet.

2.4. Future versions

This chapter presents an overview of the regulations known at the time of publication. As new requirements emerge, future editions will update the regulatory overview and the security analysis accordingly. Given the continual evolution of security, subsequent editions will also broaden the scope of the next chapter to reflect - for example - newly discovered vulnerabilities.

3. Guidance for both Charging Stations and Charging Stations Management Systems

3.1. Introduction

In this chapter — and in Chapters 4 and 6 — security measures for Charging Stations (4) and Charging Station Management Systems (6) are described. The OCPP specification defines security in dedicated sections (for OCPP 2.x: Functional Blocks A, L, and M; for OCPP 1.6: the Security Whitepaper “Improved security for OCPP 1.6-J”). Items identified as part of OCPP (marked as "*About the OCPP specification*") are mandatory for compliant implementations and are covered by the OCPP Certification Program. A way to check that these security requirements are met is to pass all relevant security test cases — either by obtaining formal certification or by running the same tests yourself with the OCPP Compliance Test Tool (OCTT). The latter has no official status (e.g. for regulators), but can help a vendor to adhere to the security requirements of OCPP.

For OCPP 1.6, the former separate Security certification has been integrated into the OCPP 1.6 Core certification as of October 2025. For OCPP 2.x, security requirements are a mandatory part of the Core; certification requires support for Security Profile 2 (TLS with Basic Authentication). For both OCPP 1.6 and 2.0.1, an Advanced Security certification profile is available for implementations that use client-side certificates for TLS (Security Profile 3).

3.2. Trustworthy Time

The following requirements related to trustworthy time apply:

Id	Requirement
SEC-0001	For many EV charging related functions, but also for basic security guarantees each Charging Station MUST have access to a trustworthy time source in a secure way.
SEC-0002	Since certificate validation, Time-based One-Time Password (TOTP) windows, log-signatures, OCSP stapling checks, and tariff/metrology evidence all depend on correct time, secure time synchronization SHALL be the first successful operation after boot before any outbound TLS control connections (excluding the time-establishment channel itself).

This last requirement implies that the Heartbeat message cannot be used as a trustworthy source of time as it is not available before an outbound control connection is set up. It is RECOMMENDED to use NTS (see also 8.2.3).

3.3. Cryptography

3.3.1. Curves for ECDSA certificates

About the OCPP specification

The security for OCPP uses X.509 certificates. At the time of writing, both RSA and ECDSA certificates are used. For security and interoperability it is important that the correct curves are used when using

ECDSA certificates.

Id	Requirement
SEC-0003	For ECDSA (based on RFC 8422) the OCPP 1.6, 2.0.1 and 2.1 specifications require that keys used are at least 224 bits long and that the secp256r1 curve (a.k.a. prime256v1) is used.

This requirement is also validated during certification. Please note that the two RSA cipher suites currently allowed SHOULD be gradually phased out because they do not support perfect forward secrecy. See chapter 7 for more information on the TLS roadmap for the future.

3.3.2. Use of FIPS-validated cryptography

About the OCPP specification

For the use of FIPS-validated cryptography, the following requirements apply:

Id	Requirement
SEC-0004	OCPP mandates TLS v1.2+, bans weak ciphers and lists strong suites that are in line with the recommendations from different governmental agencies (ECDHE_ECDSA / RSA with AES-GCM).
SEC-0005	Endpoints MUST terminate on bad TLS versions/ciphers
SEC-0006	CMMC Levels 2 & 3 do mandate to use FIPS-validated cryptography (modules/algorithms) for protecting CUI.
SEC-0007	The JC-STAR 1 requires that "*the product shall use best practice cryptography to communicate securely.*"

OCPP does not require FIPS validated crypto modules.

3.3.3. Key updates

For key updates, the following requirements apply:

Id	Requirement
SEC-0008	Keys and other credentials SHALL be regularly updated.
SEC-0009	For the CSMS certificate, OCPP RECOMMENDS fast expiration.
SEC-0010	For other keys and credentials, the update frequency SHOULD be based on a risk assessment. It is RECOMMENDED to update them at least once per year. Please note that the Charging Station will automatically try to renew its client certificate when it is going to expire (which includes generating a new public / private key pair).

3.4. Avoid use of unencrypted, unauthenticated FTP, HTTP for log file uploads and firmware downloads

Upcoming OCPP specification updates (errata & additions)

In OCPP log file uploads and firmware downloads are done via a connection separate from the OCPP WebSocket connection, via a file transfer. For this, the OCPP specification has a number of file transfer protocols that can be specified via the "FileTransferProtocols" variable.

Id	Requirement
SEC-0011	For a secure implementation - to prevent compromise through auxiliary file-transfer channels - a vendor SHALL send the firmware encrypted[7] to the Charging Station.

This can either be done by using a secure protocol (such as HTTPS, SFTP, or FTPS) to send the firmware, or by encrypting the firmware itself before sending it.

Id	Requirement
SEC-0012	In addition, the firmware MUST be signed to protect its integrity (see 4.8).
SEC-0013	A Charging Station SHALL NOT install firmware or execute code without sufficiently verifying the origin and integrity.

As for the file transfer for a firmware update, the following requirements apply:

Id	Requirement
SEC-0014	It is RECOMMENDED to use HTTP**S** for future-proofing and simplifying security.

The FTP attack surface can be larger when a vendor supports unnecessary commands.

Id	Requirement
SEC-0015	If FTP is used, the FTP commands MUST be limited and a secure transport channel SHALL be used.
SEC-0016	When using SFTP (SSH) for file transfer or log retrieval, only public key–based authentication SHOULD be allowed.
SEC-0017	It is RECOMMENDED to completely disable password and challenge-response authentication methods to prevent brute-force or phishing-based credential attacks.
SEC-0018	The SSH login SHALL NOT give an interactive shell on the server, and SHALL only give file upload (and optionally download) functionality, to prevent remote code execution on the server once access to a Charging Station is gained.

In addition to standard key-based authentication, SSH provides a native certificate-based authentication mechanism, distinct from X.509 but conceptually similar. This mechanism supports fine-grained restrictions directly embedded in the SSH certificate, such as limiting valid principals, permitted commands, source addresses, and validity periods. For larger Charge Point Operators (CPOs) operating central logging, provisioning, or PKI infrastructure, adopting SSH certificates can significantly simplify key management, support short-lived credentials, and enforce granular operational policies.

Id	Requirement
SEC-0019	To ensure integrity of the SSH connection itself, strict host key checking SHOULD be enabled on the client side.

This enforces that the Charging Station only connects to servers with a known and trusted host key, effectively preventing man-in-the-middle attacks or malicious DNS redirections.

Id	Requirement
SEC-0020	To avoid operational issues during the first connection (trust-on-first-use problem), the host key verification SHOULD NOT rely on manual acceptance but instead SHOULD use one of the following trust anchors: - CA-Signed SSH Host Certificates – use an internal SSH Certificate Authority to sign host keys; clients verify the CA's public key rather than each individual host key. - DNS-Based Host Key Verification (SSHFP Records) – publish and validate SSHFP resource records via DNS[8], enabling automated and authenticated retrieval of host key fingerprints.

3.5. Use of CommonName vs SAN

Upcoming OCPP specification updates (errata & additions)

OCPP 2.1 requires that the CSMS uses the Common Name (CN) field in its certificate to identify itself to the Charging Station.

Id	Requirement
SEC-0021	The Charging Station is required to check that the CN matches the CSMS's FQDN (requirements A00.FR.309 and A00.FR.412).

The reason to use the CN was that only one host name was expected to be used per CSMS.

The OCPP 2.1 identification policy is different from that which most browsers now use on the internet, which is for the client to only check the Subject Alternative Name (SAN). The browser's policy is stricter than specified in some standards. RFC 5280 and RFC 6125 require the SAN to be used when it is present but allow to fallback to the CN if it is not. Browsers will now however give an error when the SAN is missing from the certificate. The newer RFC 9525, which obsoletes RFC 6125, recommends against the use of the CN.

Id	Requirement
SEC-0022	In future versions of OCPP (after OCPP 2.1), the Charging Station is required to check the SAN.

3.5.1. Advantages and disadvantages

Using the SAN would have the following advantages:

- Using the standard approach used on the internet will make it easier for developers to implement using standard TLS libraries.
- Checking the SAN would not create security risks, as long as the PKI is set up properly. The PKI should ensure that the link between the CSMS and subject alternate name is verified before it

provides a certificate. This is already the normal way of working for PKIs used on the internet.

- Backwards compatibility can be provided by also putting the FQDN of the CSMS in the CN. Charging stations using an older CSMS version will check this CN and still be able to authenticate to the CSMS.

The only note of caution would be to not allow multiple host name in the SAN unless there is a clear use case for it. In principle, the CSMS could use multiple host names and put these in the SAN in a secure way. But allowing multiple host names could lead to less secure certificate management practices. For instance, CPOs could create only one certificate for multiple physical servers and then manually move the private key between them. Doing so would increase the risk that the private key gets compromised. Using multiple host names in the SAN could also create backwards compatibility problems. Charging stations that use OCPP 2.1 or older will check the CN, which only contains one host name. If the Charging Station is configured to connect to a host name that is in the SAN but not in the CN, it will refuse to connect. The reason for the connection problem may not be clear to the CPO.

Note: The use of wildcard certificates in the SAN has been analyzed separately. The conclusion of the analysis and discussion was to not allow wildcard certificates.

3.5.2. Implementation options

There would be two options for implementing identification of the CSMS through the SAN in OCPP:

- Option A: the Charging Station only checks the SAN. When no SAN is present in the certificate, it refuses the connection. The CN is ignored.
- Option B: the Charging Station first checks the SAN. If no SAN is present, it checks the CN.

The chosen option is to follow option B in future version of OCPP as option A is not backwards compatible.

Both options are compatible with the standards (RFC 5280, RFC 6125). Modern browsers follow option A. But commonly used TLS libraries however follow option B by default:

- OpenSSL allows the verification to be controlled through flags. X509_CHECK_FLAG_ALWAYS_CHECK_SUBJECT causes the subject CN to be checked even when a SAN is present. X509_CHECK_FLAG_NEVER_CHECK_SUBJECT suppresses the CN check, so that only the SAN is used. Default behaviour for OpenSSL is to first check the SAN and then the CN, as in option B.
- Mbed TLS and wolfSSL also follow option B by default. The verification cannot be changed through flags. Users would have to write a custom verification callback function.

As one of the goals of the change is to allow easier implementation using TLS libraries, option B is chosen.

The other advantage of option B is that it provides backwards compatibility with OCPP 2.0.1 and OCPP 2.1. A Charging Station that uses the SAN authentication will still connect to a CSMS that only uses the CN in its certificate.

3.5.3. Identifying the OCPP service in the SAN

The SAN allows four types of identifiers for servers (see RFC 9525):

- DNS-ID: A subjectAltName entry of type DNSName.
- IP-ID: A subjectAltName entry of type IPAddress.
- SRV-ID: A subjectAltName entry of type otherName whose name form is SRVName.
- URI-ID: A subjectAltName entry of type uniformResourceIdentifier.

Future OCPP version (after OCPP 2.1) will specify which identifiers are allowed and not allowed (see the section *"Designing Application Protocols"* in RFC 9525).

OCPP implementations can use the DNS-ID as the default option (also for interoperability reasons). Using the DNS-ID is closest to the current OCPP specification using the Common Name and hence will be easiest to implement. RFC 9525 also recommends using the DNS-ID as a baseline for interoperability.

The other three identifiers could also be allowed if there is a clear use for them:

- URI-ID could be used to point to the exact URI of the OCPP service, not just to the whole CSMS server. So, it provides more precise identification.
- IP-ID could be used when Charging Stations use a fixed IP address to connect the CSMS. But special care should be taken to mitigate risks in this case. IP addresses can be spoofed. Many Charging Stations will be connected to private networks, and then the IP address does not really identify the server. The same IP address would refer to different servers on different private networks.
- Using the SRV-ID would require adding SRV records to the DNS servers used for the CSMS. It could be added if OCPP users use SRV records. RFC 9525 recommends that application layer protocols such as OCPP specify that identifiers are not supported if they are not used.

3.6. Secure coding

OCA recommendations beyond OCPP

For secure coding the following requirements apply:

Id	Requirement
SEC-0023	The Charging Station manufacturer SHALL ensure that their developers receive sufficient training on secure development.
SEC-0024	The previous requirement also applies for CSMSs, regardless of whether it is developed in-house, purchased as a product, or provided as a service.
SEC-0025	Developers SHALL be made aware of common vulnerabilities in the technologies used and learn how to prevent introducing these.

SEC-0026	When coding in a language that is not memory safe, such as C or C++, developers SHALL in particular learn how to avoid input validation vulnerabilities such as buffer overflows.

Many real-life vulnerabilities that are found result from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length buffer. Tools are available to detect (potential) memory safety related issues in code.

Id	Requirement
SEC-0027	It is RECOMMENDED to use tools for detecting (potential) memory safety related issues in code as part of the development process for languages that are not memory safe.
SEC-0028	In all programming languages developers SHALL learn how to avoid vulnerabilities such as (OS) command injection, SQLi vulnerabilities, Server-Side Request Forgery (SSRF) and - if used on a charger - learn how to avoid common vulnerabilities in web portals (e.g. OWASP Top 10: https://owasp.org/Top10/, Cross Site Scripting (XSS), Cross-Site Request Forgery (CSRF)).
SEC-0029	Input validation on files (e.g. firmware updates) is essential. Similarly, it is RECOMMENDED to sanitize external input that is "transported" by OCPP such as ISO 15118 EXI data.
SEC-0030	CSMSs SHALL apply strict schema validation for all incoming OCPP messages, rejecting malformed or unexpected payloads.
SEC-0031	All input fields SHALL be sanitized to prevent code injection and command execution.
SEC-0032	Dynamic evaluation of content within messages SHALL be disabled.

3.7. Security testing

OCA recommendations beyond OCPP

For Security testing the following requirements apply:

Id	Requirement
SEC-0033	Manufacturers SHALL perform in-house security testing and reviews during development.
SEC-0034	The previous requirement also applies for CSMSs, regardless of whether it is developed in-house, purchased as a product, or provided as a service.

SEC-0035	It is recommended to use a combination of the following activities: - Using static code analysis tools to find input validation errors - Using software composition analysis tools to find vulnerabilities in libraries and other dependencies - Performing fuzzing on OCPP and other EV specific protocols to find input validation errors - Performing code reviews on security - Performing web penetration tests on any web interfaces - Organizing periodic penetration tests by independent parties
SEC-0036	CMMC (for Level 3 only) has a requirement to conduct penetration testing at least annually or when significant security changes are made to the system, leveraging automated scanning tools and ad hoc tests using subject matter experts.

4. Guidance for Charging Stations

This chapter contains guidance for OCPP Charging Stations to create a secure OCPP implementation. This chapter re-uses some concepts from Chapter 3, but applies them specifically to Charging Stations. Where concepts overlap, this chapter focuses on role-specific responsibilities.

4.1. Risk assessment

OCA recommendations beyond OCPP

The following requirements regarding Risk assessment apply:

Id	Requirement
SEC-0037	Manufacturers SHALL perform a risk assessment for their Charging Station to determine what security measures should be implemented. Guidance on risk assessments can for instance be found in ISO/IEC 27005 and IEC 62443-3-2.
SEC-0038a	The European Cyber Resilience Act (CRA), ENCS security requirements and NIS2 require manufacturers to perform cybersecurity risk assessment and to take the results into account during the entire lifecycle of the product.
SEC-0038b	The risk assessment SHALL take into account the intended purpose and reasonable foreseeable use of the Charging Station.
SEC-0038c	The risk assessment SHALL be used to determine whether the essential cybersecurity requirements relating to the properties of products (Annex I part I) apply to the Charging Station and how they should be implemented.

4.2. Use of Security Profiles

About the OCPP specification

OCPP specifies 3 security profiles. Security Profile 1 - Unsecured Transport with Basic Authentication Profile - by itself is not secure. It does not include authentication for the CSMS, or measures to set up a secure communication channel. Therefore:

Id	Requirement
SEC-0039	A Charging Station SHALL NOT use Security Profile 1 in untrusted networks.

It was included in the OCPP specification to be used in networks where there is a VPN between the CSMS and the Charging Station, but this means that the entire security depends on this network configuration. In case that this is the only security measure, a misconfiguration (or stolen SIM card) will make the CSMS and possibly all Charging Stations in the network vulnerable. For this reason:

Id	Requirement
SEC-0040	For field operation it is strongly advised against using a security profile without TLS.

For regulations, the following requirements for using security profiles with TLS apply:

Id	Requirement
SEC-0041	Using a security profile with TLS is linked to the legal obligations in the RED delegated act (EN_18031-1/2/3). Note: The requirement applies to *all* network interfaces, defined as an *"external interface enabling the equipment to have or provide access to a network"*. Manufacturers SHOULD therefore carefully check which interfaces on a Charging Station should be considered network interfaces.
SEC-0042	CMMC Levels 2 & 3 require the protection of communications in transit from disclosure and modification. In OCPP, this is aligned only if Security profile 2 or 3 are used.
SEC-0043	The JC-STAR requires that products use best practice cryptography to communicate securely and must protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces. This implicitly rules out Security Profile 1.

The California Consumer Privacy Act (CCPA) requires that businesses must implement *"reasonable security procedures and practices appropriate to the nature of the personal information"* to protect against unauthorized access, destruction, use, modification, or disclosure. Breaches of nonencrypted data expose businesses to liability. Although the description of the security measures is quite broad, this implies that:

Id	Requirement
SEC-0044	For the CCPA Security Profile 2 or 3 MUST be used.

Please also note that using OCPP 2.x without implementing Security Profile 2 (TLS with Basic Authentication) and optionally 3 (TLS with client-side certificates) is only allowed during development and debugging and NOT for production.

4.3. Security Profile downgrades

About the OCPP specification

There are a number of requirements in Functional Block A of Part 2 of the OCPP specification[9] related to downgrading the security profile of a Charging Station, to a less secure profile, which is summarized below:

Id	Requirement
SEC-0045	Downgrading the security profile of a Charging Station is - for security reasons - NOT RECOMMENDED.
SEC-0046	The Charging Station SHALL only allow lowering the security profile if the variable `AllowSecurityProfileDowngrade` is implemented and set to true. In that case, the Charging Station SHALL only allow to downgrade from profile 3 to profile 2.
SEC-0047	Thus a Charging Station SHALL NOT allow downgrading from profile 2 or profile 3 to profile 1 using the OCPP protocol. The reason is that this might compromise the connection if no other transport security is used.

SEC-0048	When a Charging Station is updated to a higher security profile and is successfully connected to the CSMS using the higher security profile, the OCPP specification requires that a Charging Station removes all NetworkConnectionProfiles with a lower security profile. This is to make sure that a Charging Station will not revert to a lower security profile when it has connection issues. If a hacker can temporarily disrupt the connection, a Charging Station SHALL thus not fall back to a lower security profile.

Downgrading security profiles from profile 3 to 2 was introduced for use cases for migrating from one CSMS to another CSMS. The new CSMS MUST either support the same security profile that a Charging Station is using or - in case that the variable `AllowSecurityProfileDowngrade` is implemented and is / can be set to *true* - it MUST at least support Security Profile 2 (as required by OCPP certification).

4.4. Storing information

4.4.1. Storing passwords

OCA recommendations beyond OCPP

Charging Stations are devices in the field and therefore it must be taken into account that these can be tampered with. If a device is accessible, a hacker might have access to the storage of the Charging Station. Therefore the following requirements apply:

Id	Requirement
SEC-0049	An implementor MUST take care that information is stored securely. The level of protection SHOULD be based on a security risk assessment. For example, storing passwords for the OCPP connection in plain text in the logging of a Charging Station can lead to hackers getting easy access to the password, that can be used to (attempt to) hack a CSMS.
SEC-0050	Passwords that users use to log in on the Charging Station, such as passwords used by engineers for local access, SHALL be stored salted and hashed. The HTTP Basic Authentication password used in Profile 2 can however not be stored hashed, as the Charging Station needs to use it. The main mitigating measure for this password is to use a unique password in each Charging Station, so that if a Charging Station is tampered with in the field only that Charging Station is affected.
SEC-0051	Whenever possible, the password SHOULD also be stored encrypted.
SEC-0052	In addition, it is HIGHLY RECOMMENDED to regularly update passwords.
SEC-0053	CMMC levels 2 & 3 require storing and transmitting only cryptographically protected passwords.
SEC-0054	EN 18031 requires secure storage of security assets and of network assets, personal data, and financial assets. The standard is, however, not explicit on which secure storage mechanisms are appropriate.

4.4.2. Storing (and sending) personal information

OCA recommendations beyond OCPP

For storing (and sending) personal information the following requirements apply:

Id	Requirement
SEC-0055	The California Consumer Privacy Act (CCPA) requires implementers to ensure that all personal identifiers (IdTokens, account/session data, charging logs) are encrypted at rest and in transit. For this reason, identifiers SHALL be pseudonymized / redacted in logs.[10]
SEC-0056	In addition, the CCPA says that consumers may limit use / disclosure of sensitive personal data. Therefore tokens, geolocation, payment references, and certificates SHALL only be transmitted via TLS-secured channels and never in plaintext. Sensitive attributes must be encrypted at rest and redacted from nonessential logs.
SEC-0057	The RED directive EN 18031-2 requires that for storing "privacy assets" persistently (i.e. personal information) equipment MUST always use secure storage mechanisms
SEC-0058	The JC-STAR requires that a user is provided with *"functionality such that user data can be erased from the product in a simple manner"*.

In the OCPP 2.x specification requirement SEC-0058 is supported by the CustomerInformation functionality.

4.5. Wildcard certificates

About the OCPP specification

For wildcard certificates the following requirements apply:

Id	Requirement
SEC-0059	Supporting wildcard certificates is not OCPP-compliant, so these SHALL NOT be used as stated in the OCPP specification. This is also verified during OCPP certification.

However, since this is not always implemented this way and it was not validated during certification until beginning of 2025, existing implementations in the field may at this moment depend on connecting to a CSMS using a wildcard certificate. To avoid newly certified systems breaking current non-compliant setups in the field, it was decided that vendors can opt to support disabling this check. To ensure that this (non-compliant!) “opt-out” is done in a standard way, an optional and not recommended configuration variable has been added to an OCPP erratum to disable the wildcard check for a Charging Station. This way vendors relying on this behavior can prevent immediate issues in the field with CSMSs that provide wildcard certificates. The variable - named `AllowCSMSTLSWildcards` - allows a Charging Station to support *non-OCPP compliant* behavior and connect to a CSMS that uses a wildcard certificate for the OCPP connection. If this variable is present in a Charging Station, it SHALL be ReadWrite so that a CSMS can enable the secure and OCPP compliant behavior. If the variable is not implemented in a Charging Station, the default - OCPP compliant - behavior is that a Charging Station rejects a connection to a CSMS that presents a wildcard certificate.

4.6. Use unique credentials during manufacturing

About the OCPP specification

For the use of unique credentials during manufacturing the following requirements apply:

Id	Requirement
SEC-0060	The Charging Station manufacturer SHALL initialize the Charging Station with unique credentials during manufacturing, so that the Charging Station is secure by default. Even when unique credentials are used, the CPO SHOULD change the credentials after commissioning.
SEC-0061	When HTTP basic authentication in combination with TLS is supported (Profile 2), the BasicAuthPassword configuration SHALL be initialized to a unique value.
SEC-0062	When client-side certificates are used for TLS, the Charging Station SHALL be provided with a unique private key and certificate. See also requirement A00.FR.801 in Part 2 of OCPP.
SEC-0063	The credentials SHOULD be generated by a cryptographic random number generator, so that they cannot be guessed by attackers. (See also requirement A00.FR.801.)

As for the security measures during manufacturing:

Id	Requirement
SEC-0064	The credentials SHOULD be installed in a secure area in the manufacturing plant, so that they cannot be leaked during installation.
SEC-0065	Access to these areas SHOULD be restricted to personnel who are needed for installing the keys and that has had a security screening.
SEC-0066	Physical security measures SHOULD be taken to prevent unauthorized access. (See also requirement A00.FR.801.)

Additional requirements that apply for the use of unique credentials during manufacturing are the following:

Id	Requirement
SEC-0067	When using HTTP basic authentication, the passwords SHOULD be transferred to the CPO or user in a secure way. Especially when passwords for a large number of Charging Stations are sent to the CPO, they SHOULD be sent encrypted.
SEC-0068	When client-side certificates are used, the private key SHALL be generated on the Charging Station and SHALL NOT leave the device as described in the applicable use cases in the OCPP Specification.
SEC-0069	Certificates SHOULD be created using a Certificate Signing Request, similar to how they are created during operations using the use cases A02 and A03.
SEC-0070	When the private key is (for commissioning / during manufacturing) generated outside the Charging Station, it SHOULD be kept confidential. It does not have to be shared with the CPO or end user.

SEC-0071	JC-STAR-1 does not require unique credentials to be set during manufacturing, but it does require that passwords are not shared across devices once the device is in use, according to the following requirement: *"Where passwords are used and, in any state, other than the factory default, all passwords shall be unique per device or defined by the user."*.

OCA recommendations beyond OCPP

For creating the initial certificates for the Charging Station there are several options:

1. Create the certificate in a third-party PKI trusted by both the manufacturer and CPO.
2. Create a certificate in the PKI of the manufacturer. The CPO will need to install a root or intermediate certificate of the manufacturer on their server to check the validity of the Charging Stations certificate. It would be recommended that the CPO puts the manufacturer's certificate on a commissioning server. The charging station then connects to this commissioning server on first installation, and that this server changes the certificate to one in the CPO's PKI before the charging station to a production CSMS. The production CSMS would use certificates from the CPO's own CA.
3. Create a certificate in the PKI of the CPO. The CPO will then need to provide the manufacturer with a way to create certificates from the public keys, for instance through certificate signing requests.

Please note that using unique credentials during manufacturing also applies to other connections besides OCPP - if used - such as SSH or a local web portal (using default passwords SHALL be avoided)[11].

4.7. Preinstalled well-known root CA certificates

About the OCPP specification

The following requirements apply to using preinstalled well-known root CA certificates:

Id	Requirement
SEC-0072	To be able to immediately use secure communication profiles with TLS, root certificates for OCPP SHOULD be preinstalled on the Charging Station.
SEC-0073	The OCPP specification recommends NOT to have preinstalled well-known root CA certificates on a Charging Station like in operating systems or browsers, such as for example a CA bundle.

The section in the OCPP specification about the Certificate Hierarchy describes that only root and intermediate certificates that are part of the Charging Station Operator hierarchy should be used for the OCPP connection. Trusting many additional well-known root CA certificates (e.g. via CA bundles) creates security risks and is therefore not advised in critical infrastructures. The largest risk would however come from nation state actors creating false certificates by compromising one of the CAs. CAs have been compromised in the past, and with a CA bundle a nation state has many CAs they can target. Moreover, compromising one CA would compromise all Charging Stations with the CA in their bundle.

The attack would hence affect all chargers using a CA bundle.

Id	Requirement
SEC-0074	For ISO 15118, the V2GRootCertificate and MORootCertificate MAY be installed using the OCPP Certificate Management use cases after the CPO has commissioned the Charging Station. The ISO 15118 certificates are not needed to set up secure communication to the CSMS and hence do not have to be preinstalled.

4.8. Secure firmware updates

About the OCPP specification

The following requirements apply to secure firmware updates:

Id	Requirement
SEC-0075	The Charging Station SHALL check the authenticity of firmware before it is installed, preferably by checking a digital signature. It SHOULD do this by using the Secure Firmware Update process provided in OCPP (use case L01 in Part 2).
SEC-0076	If this process is not used, other measures to check the firmware authenticity SHALL be taken, regardless of whether a firmware update is deployed over the air (OTA) or installed locally by an engineer, for instance at the operating system level.

OCA recommendations beyond OCPP

Id	Requirement
SEC-0077	To protect against local tampering with the firmware, the Charging Station SHOULD use a secure boot process if its hardware supports it. The secure boot process checks the authenticity of the firmware every time the Charging Station is booted. Secure boot is needed to conform to requirement [GEC-8] in EN 18031-3.
SEC-0078	In addition the Charging Station SHALL not allow downgrading the firmware, that is installing firmware versions older than the installed firmware. Not allowing downgrades prevents attackers from installing firmware with a known vulnerability that was fixed in later firmware versions.
SEC-0079	It is RECOMMENDED to encrypt a firmware file, to prevent exposing sensitive information that is part of the firmware (e.g. credentials).
SEC-0080	The JC-STAR requires that when the device is not constrained[12], it SHALL have an update mechanism for the secure installation of updates. When the product implements an update mechanism, the product SHALL use best practice cryptography to facilitate secure update mechanisms. In case of remote updates (via network interface), the product SHALL verify the authenticity and integrity of each update via a trusted relationship.

4.9. Secure storage mechanisms

OCA recommendations beyond OCPP

The following requirements apply to secure storage mechanisms:

Id	Requirement
SEC-0081	When a Charging Station is installed in an uncontrolled environment, it is vulnerable to physical attacks. In that case, measures SHALL be taken to protect the confidentiality and integrity of information stored on the Charging Station.
SEC-0082	As a minimum measure, the casing of the Charging Station SHALL be protected against tampering.
SEC-0083	The casing SHOULD be hardened against physical tampering, doors SHOULD be locked, and there SHALL be a sensor to detect if they have been opened.
SEC-0084	The Charging Station SHALL be configured by default to send any tamper detection events to the CSMS using the Security Event Notification use case (A04).
SEC-0085	Additional measures for secure storage SHOULD be applied when feasible and based on a risk assessment. These include:
SEC-0085a	Storing cryptographic keys in tamper resistant chips, such as TPMs or secure elements.
SEC-0085b	Encrypting the storage (drive encryption).
SEC-0085c	Disabling unused hardware ports and debug ports on the circuit boards.

4.10. Local Security log

OCA recommendations beyond OCPP

For the local security log in a Charging Station, the following requirements apply:

Id	Requirement
SEC-0086	OCPP requires that Charging Stations store events in a local security log (requirement A04.FR.04 in Part 2).
SEC-0087	The log events SHALL include a timestamp.
SEC-0088	The Charging Station SHALL take measures against failures in the security log. For instance when the log is full, the oldest entries could be discarded.
SEC-0089	A minimum number of the latest events SHALL be stored to allow investigations into incidents to be carried out effectively. The Charging Station SHOULD be able to store events for at least a week under normal operations.
SEC-0090	Logs SHALL also be protected against alteration.
SEC-0091	Secure storage measures SHOULD be used to protect against physical tampering (see Section 4.9).

SEC-0092	On human user interfaces, such as local maintenance interfaces, access to the logs SHOULD be protected as much as possible.
SEC-0093	To make the analysis of logs easier, the time on the Charging Station SHALL be synchronized.
SEC-0094	The time source integrity SHALL be protected. Please refer to 3.2 for time synchronization through OCPP heartbeat messages (vs. NTS). For other time synchronization methods, such as GPS, mobile networks, and radio transmitters, additional measures may be required.

4.11. Vulnerability handling

OCA recommendations beyond OCPP

The following requirements apply to vulnerability handling:

Id	Requirement
SEC-0095	Manufacturers SHALL set up a process to handle vulnerabilities found in the Charging Station or its dependencies.
SEC-0096	To comply with the upcoming European Cyber Resilience Act (CRA) and the ENCS security requirements (ENCS requirements), the vulnerability handling process SHALL cover:
SEC-0096a	Identifying vulnerabilities
SEC-0096b	Creating a software bill of materials for the charging station in a commonly used and machine-readable format covering at least its top-level dependencies.
SEC-0096c	Remediating vulnerabilities without delay, including providing security updates
SEC-0096d	Performing regular and effective security tests and reviews
SEC-0096e	Publicly disclosing information about vulnerabilities once they have been fixed and informing users about them
SEC-0096f	Putting in place a policy of coordinated vulnerability disclosure (and making it accessible, for example via [RFC9116])
SEC-0096g	Facilitating information sharing about vulnerabilities, for instance by providing an address where vulnerabilities can be reported
SEC-0096h	Securely distributing security updates
SEC-0096i	Ensuring security updates are distributed without delay, accompanied with an advisory message, and unless otherwise agreed free of charge

More guidance on implementing vulnerability handling and disclosure can be found in the ISO/IEC 30111 and ISO/IEC 29147 standards.

Id	Requirement

SEC-0097	To comply with the Radio Equipment delegate act (see RED Directive), the charging station SHALL be made available on the market without any publicly known exploitable vulnerabilities that would affect network, privacy, financial or security assets at the moment the Charging Station is placed on the market.
SEC-0098	To comply with JC-STAR, a manufacturer SHALL make a vulnerability disclosure policy publicly available. Requirement 2-1 states that this policy shall include, at a minimum: - Contact information for the reporting of issues; and - Information on timelines for: → initial acknowledgement of receipt; and → status updates until the resolution of the reported issues.

4.12. Hardening Charging Stations

OCA recommendations beyond OCPP

For hardening of Charging Stations, the following requirements apply:

Id	Requirement
SEC-0099	The Charging Stations SHALL be hardened by disabling any unused functionality.
SEC-0100	Charging Stations SHALL be delivered by the manufacturer in a hardened and secure configuration.
SEC-0101	The following hardening measures are recommended:
SEC-0101a	Disabling all unused network interfaces and other hardware ports on the outside of the Charging Station and if used, secure these interfaces / ports.
SEC-0101b	Disabling unused network services on each enabled network interface. Services that are only used on specific interfaces should *only* be accessible on those interfaces. This can be achieved by implementing a firewall that blocks open ports on specific interfaces where that service does not need to be accessible, or by configuring services to only listen on a specific network interface, and not all interfaces.
SEC-0101c	Allowing users to disable any optional network services and hardware ports
SEC-0101d	Wireless communication such as WiFi and Bluetooth SHALL be disabled by default whenever possible. When wireless communication is needed, it SHALL be hardened and secured according to the best practices of the protocol used.
SEC-0101e	Enabling security settings on the compiler according to best practices
SEC-0101f	Enabling the security feature "No-Execute (NX)" if available on the platform
SEC-0101g	Enabling the security feature "Write-xor-execute (W^X)" if available on the platform
SEC-0101h	Enabling the security feature "Address Space Layout Randomization (ASLR)" if available on the platform
SEC-0101i	Enabling all other security features that are available on the hardware and software platform

SEC-0101j	Do not expose internal services on the charging cable's High Level Communication interface
SEC-0101k	Do not run local Charging Station web interfaces or OCPP services with root access
SEC-0101l	When Charging Stations can be locally configured, sensitive information must be protected behind a secure login screen.
SEC-0102	The manufacturer SHALL provide documentation on how users can harden the Charging Station.
SEC-0103	The documentation provided by the manufacturer SHALL include all hardware ports, network interfaces, and network services that are enabled in the factory default state.
SEC-0104	JC-STAR requires that all unused network physical interfaces and logical interfaces SHALL be disabled.

4.13. Access control for local maintenance

OCA recommendations beyond OCPP

For access control for local maintenance, the following requirements apply:

Id	Requirement
SEC-0105	Charging Stations SHALL implement access control for engineers performing local maintenance.
SEC-0106	Charging Stations SHOULD use role-based access control.

Each engineer logs in with an individual account with unique credentials. In this way, user actions can be traced to individual users and a strong password policy can be enforced. The Charging Station checks the roles assigned to the engineer and assigns their access rights accordingly, so that the principle of least privilege can be implemented.

Most Role Based Access Control (RBAC) implementations however require that the Charging Station connects to a central access control server to get information about the engineers. So, RBAC on the Charging Station may not be feasible in every architecture. As an alternative part of the RBAC could be implemented on the laptop that the engineer uses for maintenance instead of on the Charging Station.

Id	Requirement
SEC-0107	If local user accounts are used, it is still recommended to have separate accounts for separate roles and to enforce the use of strong passwords to protect against brute-force attacks.
SEC-0108	JC-STAR requirement 5-5 states: *"Product functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication."*.

4.14. Network resilience

OCA recommendations beyond OCPP

For Network resilience the following requirements apply:

Id	Requirement
SEC-0109	If the Charging Station integrates a modem to connect to a wireless network, manufacturers SHALL ensure that the Charging Station is sufficiently resistant against denial-of-service (DoS) attacks.
SEC-0110	A firewall in the modem or Charging Station SHOULD be used to protect flooding and to ensure that DoS attacks do not affect the ongoing charging sessions.

A local controller that connects multiple Charging Stations to a CSMS may need to take additional measures to secure that communication.

Id	Requirement
SEC-0111	If the local controller is seen as a network device under EN 18031, it SHALL implement also traffic control and network monitoring to detect DoS attacks.

4.15. Backups and recovery

OCA recommendations beyond OCPP

For backups and recovery the following requirements apply:

Id	Requirement
SEC-0112	Manufacturers SHALL provide a mechanism to securely recover a Charging Station after a cybersecurity incident.
SEC-0113	Charging Stations usually do not need to have a backup capability. Data that needs to be stored long term, such as transaction and logging data, is usually only buffered for a short time on the Charging Station before it is sent to the CSMS. So, most CPOs do not need to have a capability to make backups of Charging Stations. However, it SHALL be possible to recover Charging Stations from a stored or known good configuration.
SEC-0114	If a factory reset function is provided, it SHOULD be prevented from abuse. Using the factory reset should only be possible for authorized users, for instance by requiring users to open the Charging Stations. Usually it should only be usable locally to prevent mass resets. Manufacturers should determine what the right policy is for the credentials on the Charging Station in a reset.
SEC-0115	CMMC levels 2 & 3 require having an "*operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.*"

5. Guidance for Charging Station Operators

This section describes organizational measures that a CPO should take to securely operate their CSMS and Charging Stations. The measures are linked to legal obligations where relevant.

5.1. Security risk assessments

OCA recommendations beyond OCPP

Regarding Security risk assessments, the following requirements apply:

Id	Requirement
SEC-0116	The CPO SHALL perform yearly cybersecurity risk assessments.
SEC-0117	The risk assessment SHALL cover all business processes related to the operation and management of the Charging Stations.
SEC-0118	Risk assessments SHALL be performed in a structured way, for instance following the ISO/IEC 27005 standard.
SEC-0119	The CPO SHALL define and document a risk assessment method and risk criteria.

Relation with regulation

When looking at current regulation, the following requirements apply:

Id	Requirement
SEC-0120	Both the NIS2 directive and the NCCS require CPOs to perform cybersecurity risk assessment to determine appropriate measures.

For NIS2, the requirements for performing a risk assessment are determined by each member state. The NCCS defined requirements for performing a risk assessment are included in Article 26. The following applies:

Id	Requirement
SEC-0121	Entities SHALL report risks on a common risk-impact matrix developed by ENTSO-E and the DSO entity. The impact metrics of this matrix are defined to measure disruption to the electricity system.

The above requirement means that CPOs will need to take impacts to the electricity system into account. CPOs only need to perform a risk assessment under the NCCS if they are identified as a high- or critical-impact entity.

The CMMC has a risk assessment section for Levels 2 & 3, for which the following applies:

Id	Requirement
SEC-0122	The CMMC requires the CPO to periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems.

A risk assessment is the basis for CPO security measures. For example, CMMC requires to scan for vulnerabilities in organizational systems and applications periodically and - when new vulnerabilities affecting those systems and applications are identified - to remediate vulnerabilities in accordance with risk assessments.

5.2. Information security management system

OCA recommendations beyond OCPP

Regarding Information security management systems (ISMS), the following requirements apply:

Id	Requirement
SEC-0123	CPOs SHALL set up an information security management system based on the ISO/IEC 27001
SEC-0124	The management system SHALL cover all business processes related to the operation and management of the Charging Stations.
SEC-0125	The management system SHOULD be certified.

Relation with regulation

Having a cybersecurity management system is often a good basis for complying with national NIS2 directive regulations. Many countries accept a certified management system as evidence for meeting the NIS2 risk management requirements.

For the NCCS the following requirements apply:

Id	Requirement
SEC-0126	CPOs that are classified as a high-impact entity under the NCCS are required to set up a cybersecurity management system. Requirements for such a management system are included in Article 32 of the NCCS. The requirements are based on the ISO/IEC 27001 standards. So, CPOs can comply by setting up a management system compliant to that standard.
SEC-0127	If a CPO is classified as a critical-impact entity, it is required to provide verification evidence of the implementation of the management system. CPOs can do this by getting their management system certified against ISO/IEC 27001. If the competent authority in a member state supports it, they could also provide verification evidence through audits by the authority or through peer reviews by other critical-impact entities.

Whether an entity such as a CPO is high- or critical-impact is determined through so-called Electricity Cybersecurity Impact Indices (ECII). The ECII measures the possible impact on the European electricity system if the entity is compromised in a cyber-attack. ENTSO-E and the DSO entity have published a set of provisional ECII.

For a CPO, the ECII is defined as the total charging capacity of all recharging points that it operates. The document also defines thresholds for when an entity would be considered high- or critical-impact for each EU member state. For instance, for countries in continental Europe, the critical-impact threshold is 3,000 MW. CPOs that are above these provisional thresholds should have been informed by their competent authority by 13 March 2025.

The real (non-provisional) ECII will be published after a Union-wide risk assessment has been performed.

5.3. Supply chain security

OCA recommendations beyond OCPP

Regarding supply chain security, the following requirements apply:

Id	Requirement
SEC-0128	CPOs SHALL set security requirements when procuring new components, systems, and services, such as Charging Stations, CSMSs, and cloud services.
SEC-0129	It is RECOMMENDED for CPOs to use the ElaadNL and ENCS security requirements (see 2.1.6) for this purpose when procuring new Charging Stations.
SEC-0130	For high-risk systems, the CPO SHALL verify the implementation of the requirements through security tests and audits.

Relation with regulation

The NIS2 directive requires entities to take supply chain security measures. The exact measures are determined on member state level.

The NCCS requires all high-impact entities to implement certain minimum cybersecurity controls, and all critical-impact entities to implement advanced cybersecurity controls. These cybersecurity controls still need to be defined. They will be developed by ENTSO-E and the DSO entity based on a Union-wide risk assessment and then need to be approved by the NCCS competent authorities. The minimum and advanced cybersecurity controls will include controls on supply chain security. The controls are meant to ensure that the procurement process at CPOs takes security into account. In particular, Level 3 of CMMC has two requirements for supply chain security:

Id	Requirement
SEC-0131	Level 3 of CMMC requires to assess, respond to, and monitor supply chain risks associated with organizational systems
SEC-0132	Level 3 of CMMC requires to develop a plan for managing supply chain risks associated with organizational systems and system components; update the plan at least annually, and upon receipt of relevant cyber threat information, or in response to a relevant cyber incident.

5.4. Key management processes

About the OCPP specification

Regarding key management processes, the following requirements apply:

Id	Requirement
SEC-0133	The CPO SHALL set up a process to manage all cryptographic keys.
SEC-0134	The process SHALL in particular describe the process for creating and updating the keys and certificates used in the OCPP protocol, as described in Functional Block A. Security, Section 1.4 - "Keys used in OCPP" of Part 2 of the OCPP specification.

In most cases, the CPO will need to use a public key infrastructure to manage certificates. OCPP uses the CSMS certificate for the authentication of the CSMS. If the CPO uses Security Profile 3, the Charging Station certificate is also used for the authentication of the Charging Station. The CPO can set up the PKI themselves as an internal process or use an external service provider.

5.4.1. Private key leakage process

About the OCPP specification

Regarding private key leakage, the following requirements apply:

Id	Requirement
SEC-0135	CPOs SHOULD set up a process to revoke certificates in case the private keys used in OCPP are compromised.
SEC-0136	The OCPP standard includes a RECOMMENDED strategy for certificate revocation in Functional Block A Security, Section 1.5 - "Certificate Revocation" of Part 2, consisting of two parts: - For the *Charging Station Certificate*, the CSMS checks the revocation status for Charging Station certificates using the Online Certificate Status Protocol (OCSP). - For the *CSMS certificate*, it is recommended that fast expiration is used, so that the compromised certificate automatically expires. In this way, the Charging Station does not have to implement Certificate Revocation Lists or OCSP. In case the private key used for signing the firmware is compromised, the Charging Station manufacturer would have to provide a firmware update to change the firmware signing certificate so that the Charging Station can perform secure firmware updates again that do not use a compromised certificate hierarchy.

5.4.2. Wildcard certificates

About the OCPP specification

For wildcard certificates the following requirements apply:

Id	Requirement

SEC-0137	Using wildcard certificates by a CSMS is not OCPP-compliant, so these SHALL NOT be used as stated in the OCPP specification. This is also verified during OCPP certification and an implementation using wildcards is thus not certifiable.

However, since this is not always implemented this way and it was not validated during certification until beginning of 2025, existing implementations in the field may at this moment depend on connecting to a CSMS using a wildcard certificate. To avoid newly certified systems breaking current non-compliant setups in the field, it was decided that Charging Station vendors can opt to support disabling this check. To ensure that this (non compliant!) “opt-out” is done in a standard way, an optional and not recommended configuration variable has been added to an OCPP erratum to disable the wildcard check for a Charging Station. This way vendors relying on this behavior can prevent immediate issues in the field with CSMSs that provide wildcard certificates. The variable - named `AllowCSMSTLSWildcards` - allows a Charging Station to support non-OCPP compliant behavior and connect to a CSMS that uses a wildcard certificate for the OCPP connection. If this variable is present in a Charging Station, it SHALL be ReadWrite so that a CSMS can enable the secure and OCPP compliant behavior.
If the variable is not implemented in a Charging Station, the default - OCPP compliant- behavior is that a Charging Station rejects a connection to a CSMS that presents a wildcard certificate.

5.4.3. Root CA key lost

OCA recommendations beyond OCPP

The following requirements related to the Root CA key apply:

Id	Requirement
SEC-0138	The Root CA private key MUST be protected with the highest level of security.
SEC-0139	It is HIGHLY RECOMMENDED to keep the Root CA offline whenever possible, preferably by storing the private key in a Hardware Security Module (HSM), and to restrict access through multi-person authorization (e.g., the four-eyes principle).
SEC-0140	CSMS and Charging Station certificates SHOULD be signed using intermediate certificates.

If the confidentiality of the Root CA private key is lost, the existing PKI can no longer be trusted as attackers, who have obtained the key, can create false certificates. In this case, the following applies:

Id	Requirement

SEC-0141	A new Root CA must be established and the CA certificates on all affected Charging Stations must be updated. Depending on the deployment, this may be achieved through one of the following mechanisms: - The "Install CA certificate" use cases over the existing OCPP connection. - Physical maintenance (e.g., USB media, a local service interface, or an on-site technician). - A firmware update signed using the Manufacturer Root Certificate. - Replacement of the Charging Station as a last resort.
SEC-0142	In addition it is HIGHLY RECOMMENDED to make backups of the root CA private key and relevant intermediate private key. If these keys are no longer available, the CA certificates on the Charging Stations SHOULD also be updated through one of the above mechanisms.

When the AdditionalRootCertificateCheck mechanism is enabled, the first option is no longer possible. This mechanism requires a newly installed Root CA to be signed by an already trusted Root CA. This could be done by a secure Root CA rollover by first installing a new Root CA certificate signed by the current Root CA, followed by installation of the self-signed version of the new Root CA as described in a recent erratum.

If the original Root CA private key is no longer available, this rollover process can no longer be performed. To mitigate this risk, it is RECOMMENDED to generate the Root CA rollover certificate in advance—while the original Root CA private key is still available—and store it securely as part of the PKI backup. This pre-generated rollover certificate can then be used to establish trust in the new Root CA, even if the original Root CA private key is no longer available.

5.5. Logging and monitoring

OCA recommendations beyond OCPP

Regarding logging and monitoring, the following requirements apply:

Id	Requirement
SEC-0143	The CPO SHALL set up a process to monitor their systems for anomalous behavior (see 5.5.4) and detect security incidents.
SEC-0144	The CPO SHALL use multiple data sources for monitoring to get the best possible visibility on the system, including logs, SecurityEvents, NotifyEvents, network traffic, and tamper detection alerts.
SEC-0145	Monitoring SHALL be performed by properly trained personnel. Usually, these work in a Security Operations Center (SOC). Larger CPOs may have a SOC in-house. Others can use SOC services from an external provider.

5.5.1. Log monitoring

OCA recommendations beyond OCPP

Regarding log monitoring, the following requirements apply:

Id	Requirement
SEC-0146	The CPO SHALL set up monitoring of the security logs of the CSMS and connected Charging Stations.
SEC-0147	Use cases SHOULD be set up to detect: - repeated failed authentications - unexpected configuration changes - commands sent outside normal operating hours - anomalous charging behavior at scale
SEC-0148	The detection use cases SHOULD be selected based on the CPO's security risk assessment.
SEC-0149	Logs SHOULD be gathered in a Security Information and Event Management (SIEM) system for analysis from all sources needed to implement the use cases, including: - Charging stations - Operating system logs - Application logs - Logs from firewalls, switches, and other network devices - Logs from security systems, such as IDS, IPS, anti-virus and endpoint protection - Logs from hypervisors and other infrastructure components
SEC-0150	The SIEM system SHOULD be used to correlate the events from all these sources.

Relation with regulations

Regarding log monitoring, the following regulatory requirement applies:

Id	Requirement
SEC-0151	CMMC Levels 2 & 3 have the requirement to create and retain system audit logs and records to the extent needed to enable the monitoring, and to ensure that the actions of individual system users can be uniquely traced to those users.

5.5.2. Network monitoring

OCA recommendations beyond OCPP

Regarding network monitoring, the following requirements apply:

Id	Requirement
SEC-0152	The CSMS SHALL implement traffic control and network monitoring on its network. These measures are especially important against (distributed) denial-of-service attacks.

SEC-0153	When using OCPP Security Profile 2 for the connection between Charging Station and CSMS, a malicious charger / hacker can perform a brute force attack to discover a combination of ChargingStationId and password. For this reason, the CSMS SHALL also monitor network traffic to take action against this type of attacks (example actions: withdrawing network level access for a malicious charger and send an engineer to repair it). By restricting network access to the CSMS to only the Charging Stations (so no public access) a CSMS can reduce this risk.

Despite this, network monitoring is required, as Charging Stations are devices "in the field" and could be tampered with (see also 5.5).

Id	Requirement
SEC-0154	When using Security Profile 2, OCPP requires a minimum password length of 16 characters.

At the time of writing the above required minimum password length is considered a strong password by for example CISA (the U.S. government Cybersecurity & Infrastructure Security Agency).

Id	Requirement
SEC-0155	A CSMS SHALL NOT accept unknown Charging Station IDs as part of the provisioning process, as this allows for an easy way to overwhelm the CSMS with fake Charging Station Ids.
SEC-0156	To prevent brute force attacks for authentication credentials, it is HIGHLY RECOMMENDED to use OCPP Security Profile 3, which makes use of client certificates instead of usernames and passwords.

When a connection is set up for a charger that already has an open websocket connection, the CSMS has 2 options. It can only accept the new connection if it determines that it cannot send messages over the old connection anymore ("*stale connection*"). However, this can be difficult to implement in a resilient, scalable CSMS environment (websocket connections could be handled by different worker nodes / load balancer servers).
Alternatively the CSMS can accept the connection at first and determine - e.g. in another module - that multiple / inconsistent connections exist for a charger. This inconsistency must then be remediated by closing superfluous connections.
In addition, the CSMS can actively monitor for frequent reconnection loops, which may indicate a malicious device fighting with the authentic one over the connection.

5.5.3. Monitoring for physical tampering

OCA recommendations beyond OCPP

Regarding physical tampering, the following requirement applies:

Id	Requirement

SEC-0157	The CPO SHALL monitor for attempts to physically tamper with the Charging Stations. Physical tampering can not only be used to commit fraud. If a Charging Station is physically compromised, it can also serve as an entry point from which to attack the CSMS.

The CPO can use the OCPP Security Event Notification (use case A04) to detect physical tampering. An event is defined in OCPP to alert when the tamper detection sensor is activated (`TamperDetectionActivated`).

5.5.4. Examples of anomalous behavior

The previous paragraphs mention anomalies. Depending on the implemented use cases by a CSMS, different behavior can be considered an anomaly. The following (non exhaustive) list gives an overview of anomalies that can be monitored for:

- Security / connection related anomalies
  - Many authentication requests in a short time
  - Many failed connection attempts to the CSMS in a short time period
  - Many CallErrors in a short time period
  - Security events or firmware status related messages for Charging Stations that are not being updated
  - Key update events or messages from Charging Station whose keys do not need to be updated
  - Unexpected time change events
  - Unexpected reboot or reset events
  - Reconfiguration of security parameter events for Charging Stations that are not being reconfigured
  - Maintenance login events (accepted or failed) at unusual times or in unusual numbers
- Transaction / billing related anomalies
  - Many concurrent transactions started with the same IdToken (specifically when concurrent transation are not allowed).
  - Use of an idToken on a different continent than expected.
  - Many authorization requests in a short time period
  - Unexpected transaction related messages
  - Duplicate sequence numbers
  - Transaction related messages for a transaction on Charging Station A, via the websocket connection of Charging Station B
  - Inconsistent meter values (e.g. a decrease in cumulative energy readings when no energy is being exported)

- Many re-used OCPP messageId or transactionIds
- Inconsistent / extreme charging limits reported by Charging Stations

5.5.5. Information sharing and incident reporting

OCA recommendations beyond OCPP

Regarding information sharing and incident reporting, the following requirements apply:

Id	Requirement
SEC-0158	The CPO SHALL set up process to report security incidents to the relevant authorities.
SEC-0159	The CPO SHOULD set up processes to receive threat and incident information from their authorities, so that they can more effectively monitor their own systems.

Relation with regulation

Regarding information sharing and incident reporting, the following regulatory requirements apply:

Id	Requirement
SEC-0160	In the EU, reporting incidents is required by the NIS2 directive and the NCCS. For NIS2, the thresholds for when incidents must be reported are defined at a national level. For the NCCS, a cyber-attack classification scale will be developed. A proposal for this scale is available at the ENTSO-E website[13].
SEC-0161	CMMC levels 2 & 3 require incident reporting, specifically to *track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.*
SEC-0162	ENCS requires that the CPO must report security incidents in its EV charging system to the purchasing party. In this case the purchaser would for instance be a local government buying services for the management of their public Charging Stations.

5.6. Vulnerability management

OCA recommendations beyond OCPP

Regarding vulnerability management, the following requirements apply:

Id	Requirement
SEC-0163	The CPO SHALL set up a vulnerability management process to identify and mitigate vulnerabilities in their systems.
SEC-0164	For the central server infrastructure, it is RECOMMENDED to set up automated vulnerability scanners to continuously monitor for new vulnerabilities. For Charging Stations or the CSMS application, vulnerability reports are usually received from their developers.
SEC-0165	The CPO SHALL set up a clear policy for prioritizing vulnerabilities and targets for mitigating them.

SEC-0166	The prioritization of vulnerabilities SHOULD be based on the risk the vulnerability poses. The risk can be determined partly based on the CVSS score of a vulnerability, but SHOULD also take into account which parts of the CSMS or Charging Station are affected, what the impact would be if these would be compromised, and how exposed they are to exploits.

5.7. Secure software development

OCA recommendations beyond OCPP

Regarding secure software development, the following requirement applies:

Id	Requirement
SEC-0167	If software is developed in-house by the CPO, for instance for the CSMS, a secure software development process SHALL be used. The process SHOULD be based on one of the following frameworks: - IEC 62443-4-1 - OWASP SAMM

5.8. Use of passwords

OCA recommendations beyond OCPP

As indicated in 4.4.1 it is HIGHLY RECOMMENDED to regularly update passwords. For a CPO the following requirements apply:

Id	Requirement
SEC-00168	Static manual passwords are a residual risk. A CPO SHALL use randomized passwords (for HTTP basic authentication) of maximum length and shall regularly (e.g. once per month) change all passwords to avoid attacks by leaked passwords. To keep the increased workload as low as possible the CPO shall rely on fully automated processes. Please note that this differs from guidelines such as NIST SP 800-63B-4, which advises not to *periodically* change *human* passwords, but only in case of evidence of compromise.
SEC-0169	As indicated in 4.6 the Charging Station manufacturer SHALL initialize the Charging Station with unique credentials during manufacturing, so that the Charging Station is secure by default. Even when unique credentials are used, the CPO SHOULD change the credentials after commissioning.

6. Guidance for Charging Station Management Systems

This chapter re-uses some concepts from Chapter 3 and 4, but applies them specifically to Charging Station Management Systems (CSMSs). Where concepts overlap, this chapter focuses on role-specific responsibilities. Please note that when securing a CSMS, a vendor must also take into account all applications that directly or indirectly access a CSMS such as related smartphone apps for managing charging sessions.

6.1. Application security

6.1.1. Access control

This section specifies requirements for access control on the CSMS for different types of users.

Human users

OCA recommendations beyond OCPP

Regarding access control for human users, the following requirements apply:

Id	Requirement
SEC-0170	The CSMS SHALL use Role-Based Access Control (RBAC) for human users.
SEC-0171	Users of the CSMS SHALL use individual accounts to log in on the CSMS.
SEC-0172	The CSMS SHALL assign users access rights based on their role, as registered in a central access control server.
SEC-0173	The CSMS SHOULD implement at least the following roles to allow implementing the principle of least privileges: - 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.
SEC-0174	The CSMS SHALL ensure that critical functions can only be performed by authorized users.
SEC-0175	To avoid problems in the electricity system, the user interface of the CSMS SHALL limit on how many Charging Stations a user can switch charging on or off simultaneously.

System users

OCA recommendations beyond OCPP

Regarding access control for system users, the following requirements apply:

Id	Requirement
SEC-0176	The control system SHALL provide the capability to separate different types of system (non-human) users.
SEC-0177	The CSMS SHOULD implement at least the following roles for other system users: - Mobility service providers - Roaming platforms - TSOs or DSOs (for smart charging) - Charging stations

6.1.2. Use of Security Profiles

About the OCPP specification

OCPP specifies 3 security profiles:

- Unsecured Transport with Basic Authentication Profile – 1
- TLS with Basic Authentication Profile – 2
- TLS with client-side Certificates Profile - 3

For field operation it is strongly advised against using a security profile without TLS, that is, it is HIGHLY RECOMMENDED to use profile 2 or 3.

Id	Requirement
SEC-0178	A CPO SHALL NOT allow the CSMS to use Profile 1 in untrusted networks.

Profile 1 by itself is not secure. It does not include authentication for the CSMS, or measures to set up a secure communication channel. It can be used in networks where there is a VPN between the CSMS and the Charging Station, but this means that the entire security depends on this network configuration. In case that this is the only security measure, a misconfiguration (or stolen SIM card) will make the CSMS and possibly all Charging Stations in the network vulnerable.

Id	Requirement
SEC-0179	For this reason for field operation it is strongly advised against using a security profile without TLS.
SEC-0180	When TLS is used – for maintenance purposes - it is RECOMMENDED to use clear internal error messages, for example using the correct TLS error when no common cipher suite is found.

Please also note that using OCPP 2.x without implementing Security Profile 2 (TLS with Basic Authentication) and optionally 3 (TLS with client-side certificates) is only allowed during development and debugging and NOT for production.

Id	Requirement

SEC-0181	As described in 4.3 , downgrading the security profile of a Charging Station by the CSMS is - for security reasons - NOT RECOMMENDED. A CSMS is required not to allow the Charging Station to connect with a lower security profile anymore.

Relation with regulations

Regarding the use of security profiles, the following regulatory requirements apply:

Id	Requirement
SEC-0182	CMMC Levels 2 & 3 require the protection of communications in transit from disclosure and modification. In OCPP, this is aligned only if Security profile 2 or 3 are used.
SEC-0183	The California Consumer Privacy Act (CCPA) requires that businesses must implement *"reasonable security procedures and practices appropriate to the nature of the personal information"* to protect against unauthorized access, destruction, use, modification, or disclosure. Breaches of nonencrypted data expose businesses to liability. Although the description of the security measures is quite broad, this implies that Security Profile 2 or 3 MUST be used for this regulation.

6.1.3. CSR verification

Upcoming OCPP specification updates (errata & additions)

When using Security Profile 3, a Charging Station requests a new certificate through a Certificate Signing Request (CSR). The CSR should be verified before the CA issues the new certificate. The two main verification steps are checking that the CSR is coming from the right Charging Station and checking the properties of the CSR.

Checking the identity of the Charging Station

Regarding checking the identity of the Charging Station, the following requirement applies:

Id	Requirement
SEC-0184	Before issuing a certificate, the Certificate Authority (CA) (it could be the CSMS that fulfills this role) SHALL check if the CSR is coming from the Charging Station for which the certificate is requested. If the identity in the CN field of the CSR does not match the identity of the Charging Station that sent the CSR, the CSR MUST be refused.

Without the check in SEC-0184, a compromised Charging Station could request certificates for other Charging Station. Once it has these certificates, it could impersonate these other Charging Stations, for instance creating fake transactions.

The identity of the Charging Station MAY be checked at the CSMS or at the Certificate Authority (CA). A check at the CSMS is easiest to implement. When Security Profile 2 or 3 is used, the CSMS has already authenticated the identity of the Charging Station when it receives the CSR, either through a password or through the old private key. The CSMS can then simply check that the identity in the CN field of the CSR matches the identity of the Charging Stations that sent the CSR.

The approach could also be used if Security Profile 1 is used, as the Charging Station still authenticates itself using a password. However, if the connection is not secured, the authentication may not be trustworthy.

The risk of checking the Charging Station identity in the CSMS, is that in case the CSMS itself is compromised, it can freely create false certificates for Charging Stations. The CA itself has no way to check if a CSR is really coming from a certain Charging Station. It fully relies on the CSMS.

To detect a compromised CSMS, the CA itself could check the identity of the Charging Station. The CA could do this if the Charging Station would sign the CSR with its old private key. The CA can then check the signature to know the CSR is coming from that Charging Station. The challenge is to provide the signed CSR in a format that the CA can easily read. One option would be to use the PKCS#7 format as is it used in the Simple Certificate Enrollment Protocol (SCEP). The methods used to check the identity in the EST or ACME protocols seem less suitable for OCPP. EST uses the authentication in the TLS connection to check the source of the CSR. So, using EST would require the Charging Station to have a direct TLS connection to the CA, bypassing the CSMS. The ACME methods are more designed for use on the web and use either domain challenges or account keys. Neither options seems easy to implement in OCPP. The implementation of checks at the CA is complex. Changes are needed in the Charging Station firmware to generate the signed CSR. And the CA needs to be configured to perform the right checks. It should be considered if the additional complexity is worth it to mitigate the risk of a CSMS compromise.

Checking the certificate properties

Regarding checking the certificate properties, the following requirement applies:

Id	Requirement
SEC-0185	Before issuing a certificate, the CSMS or the Certificate Authority (CA) SHALL check the properties in the certificate against the relevant TLS policy. This includes checking: - The key lengths - The presence of required fields such as the serial number and organization name - The format of the SAN and CN fields - The use of the key usage extension with the correct usages

The checks on the certificate properties could be performed at the CSMS, but preferably the checks should be done on the CA side, as it is the most trusted part of the system.

6.1.4. Firmware updates

Upcoming OCPP specification updates (errata & additions)

Regarding firmware updates, the following requirements apply:

Id	Requirement
SEC-0186	The CSMS SHALL support automated updates of Charging Station firmware to allow for the efficient installation of security updates. Charging Stations are required to support secure firmware updates as part of OCPP Certification.

SEC-0187	Measures SHOULD be in place to ensure that the updates do not disrupt the operations of the Charging Stations, for instance by using a gradual, phased rollout process.
SEC-0188	The CSMS SHALL ensure that firmware updates can only be performed by authorized users.

Relation with regulations

Regarding firmware updates, the following regulatory requirements apply:

Id	Requirement
SEC-0189	The harmonized standard for the Radio Equipment Directive (EN 18031) has a requirement for automated firmware updates. This is formally a requirement to the Charging Station. But it would be RECOMMENDED to support it through the CSMS.

6.1.5. Protecting against DoS attacks through the TLS client-certificate validation

OCA recommendations beyond OCPP

Some certificate extensions ask the CSMS to look up intermediate certificates, certificate revocation lists or other information on external servers. Attackers could abuse such extensions to perform denial-of-service attacks.

For instance, certificates could contain an Authority Information Access (AIA) extension pointing to a URL where intermediate certificates can be fetched. Attackers can point this URL to a slow or unresponsive server. This could result in TLS connections being kept open. By repeating this attack the CSMS could run out of resources.
The risk of such attacks is highest when the CSMS is exposed to the internet or other untrusted networks.

Therefore the following requirements apply:

Id	Requirement
SEC-0190	The CSMS SHALL implement measures to protect against denial-of-service (DoS) attacks.
SEC-0191	The measures to protect against DoS attacks SHOULD include: - Setting strict timeouts on requests to external servers such as AIA fetch requests - Pre-loading or caching the requested information such as intermediate certificates - Whitelisting the external servers for instance by setting the allowed AIA hosts
SEC-0192	Where possible, AIA fetching SHOULD be disabled entirely and the intermediate certificates SHOULD be preloaded on the CSMS.

6.2. Platform security

6.2.1. Cloud platform certifications

OCA recommendations beyond OCPP

If the CSMS is run on a cloud platform, the following requirement applies:

Id	Requirement
SEC-0193	The platform SHOULD be certified for security through one of the following certifications[14]: - SOC 2 - FedRAMP - CSA STAR - EU Cloud Services (EUCS) (when available) - ISO/IEC 27001 with the cloud-specific ISO/IEC 27017 controls

6.2.2. Measures against denial-of-service attacks

OCA recommendations beyond OCPP

Besides protecting the CSMS against denial-of-service attacks on the application level as discussed in 6.1.5 , the following requirement applies for denial-of-service attacks on the CSMS platform level:

Id	Requirement
SEC-0194	Measures SHALL be implemented to protect the CSMS from denial-of-service (DoS), including distributed denial-of-service (DDoS) attacks.

DoS can come from any outside interfaces, such as portals exposed on the internet, connections to other servers, or from Charging Stations in the field. Example measures against DDoS attacks are proxies, traffic-filtering tools, distribution of data centers over different locations and additional layers of redundancy in DNS servers.

6.2.3. Physical redundancy

OCA recommendations beyond OCPP

To protect against natural disasters or power outages, the following physical redundancy requirement applies:

Id	Requirement
SEC-0195	The need to have physical redundancy SHOULD be analyzed for a CSMS to protect against natural disasters or power outages. Redundancy can be provided through the cloud platform. It is important that the redundant locations can communicate with the Charging Stations.

6.2.4. Secure storage

OCA recommendations beyond OCPP

For the storage of keys, the following requirements apply:

Id	Requirement
SEC-0196	The platform SHALL store private keys and symmetric keys in a secure environment.
SEC-0197	Where possible, keys SHOULD be protected through the use of a Hardware Security Module (HSM) or comparable technology.

As indicated in 4.4.2, the California Consumer Privacy Act (CCPA) requires implementers to ensure that all personal identifiers (IdTokens, account/session data, charging logs) are encrypted at rest and in transit. For CSMSs this implies the following requirement:

Id	Requirement
SEC-0198	The CSMS SHALL encrypt confidential data at rest, including personal identifiers.

6.3. Defense in depth

OCA recommendations beyond OCPP

In practice, not all Charging Stations and CSMSs implement OCPP Security Profiles 2 or 3 correctly (or not implement security at all). In addition, as shown by researchers during hacker competitions, some Charging Stations can be hacked and control of these chargers can be taken over. This creates situations in which researchers, or potentially malicious actors, are able to test / exploit unexpected or invalid inputs at the CSMS. This section provides a number of recommendations for additional validation measures that should be considered when developing or operating a CSMS. Even when OCPP security mechanisms are in place, a single malicious or compromised Charging Station may be able to exploit missing validations that may initially appear unnecessary or redundant.

Id	Requirement
SEC-0199	To control the impact of a malicious Charging Station on a CSMS, each Charging Station MUST be isolated from other Charging Stations in the network, as well as on application level in the CSMS (e.g. "sandboxing").
SEC-0200	On the network level the following is RECOMMENDED: - Local WiFi network: Clients SHOULD only be able to connect to the CSMS and SHOULD NOT be able to communicate directly with other clients. - VPN / APN mobile network: Clients SHOULD only be able to connect to the CSMS and SHOULD NOT be able to communicate directly with other clients. - Ethernet / internet: The CSMS SHOULD enforce isolation between Charging Station connections and SHOULD NOT allow one Charging Station to communicate with or affect another Charging Station through the CSMS infrastructure.

In addition, the following recommendations apply:

In OCPP the messageId in a message must be unique per Charging Station, except for resent messages (which are likely to occur in case of bad network connections). Uniqueness cannot be guaranteed over different Charging Stations. For this reason the following applies:

Id	Requirement
SEC-0201	A CSMS SHALL not use the messageId of OCPP messages as a primary key for storing / processing messages. This prevents overwriting information by different chargers using the same Ids and also prevents data loss in case a malicious Charging Station sends messages to the CSMS.

Similarly transactionIds are not unique in OCPP 2.x as these are determined by the Charging Station. For this reason:

Id	Requirement
SEC-0202	A CSMS MUST link transaction related information to a specific Charging Station (or even connection) and SHALL not consider transactionIds to be unique. This prevents loss of data in case of a malicious Charging Station re-using transactionIds.
SEC-0203	In general, messages that are received from a Charging Station SHALL not overwrite existing data in the CSMS as this can cause loss of data in case of a malicious Charging Station. As rejecting might lead to unwanted resend behavior, this should not be rejected, but accepted and SHOULD be flagged as an anomaly.
SEC-0204	When a Charging Station sends messages for a transaction that are not expected - for example after closing the transaction - these SHALL NOT overwrite existing data and SHOULD be marked as an anomaly. This is to prevent a malicious Charging Station to alter transaction data after a transaction was stopped, by reusing a closed TransactionId.

In some cases a CPO wants to allow an IdToken to be used on different Charging Stations at the same time; in other cases this is considered unwanted behavior. The OCPP specification can be used for both implementations, but this does require the implementer to be aware of the behavior that a CPO considers to be (un)wanted.

Id	Requirement
SEC-0205	In case the choice is made not to support concurrent transactions for an IdToken, a validation for concurrent transactions MUST be in place at the CSMS. The OCPP specification offers a specific reason `ConcurrentTx` for rejecting an authorization request because of another running transaction.

7. TLS versions and security policies

Upcoming OCPP specification updates (errata & additions)

OCPP uses Transport Layer Security (TLS) for secure communication. The TLS protocol is continuously updated through the release of new protocol versions and by adding and deprecating cipher suites. This impacts the OCPP protocol and this chapter explains how updates will be handled in the future for both Charging Stations and Charging Station Management Systems.

7.1. Expected updates to TLS

Based on government recommendations, updates in OCPP are expected related to upgrading to TLS 1.3, deprecating the currently used RSA cipher suites, and implementing post-quantum algorithms.

7.1.1. TLS version 1.3

The use of TLS 1.3 is already allowed in OCPP 2.0.1 and 2.1. The requirements allow TLS 1.2 and any newer version.

Id	Requirement
SEC-0206	It is RECOMMENDED to always use TLS 1.3 if both the CSMS and the Charging Station support this.

This is already standard behavior for most TLS implementations.

At a certain point in time it will no longer be allowed to use TLS 1.2. At the time of writing there is no urgent need for this. There are no official timelines for phasing out TLS 1.2 and it is still widely used. When properly configured as it is in OCPP, there are also no known vulnerabilities in TLS 1.2.

However, as standard development takes time and Charging Stations have a long lifetime, this chapter focuses on preparing implementations for TLS 1.3 in OCPP early[15].

Id	Requirement
SEC-0207	It is RECOMMENDED that any Charging Station developed after the release of this whitepaper is prepared for using TLS 1.3 to make it forward compatible when TLS 1.3 becomes the norm.

7.1.2. Phasing out cipher suites without perfect forward secrecy

For the two RSA cipher suites in OCPP, the following applies:

Id	Requirement
SEC-0208	The two RSA cipher suites currently allowed SHOULD be gradually phased out because they do not support perfect forward secrecy.

OCPP 2.0.1 and 2.1 support both elliptic curve and RSA cipher suites. The RSA cipher suites are:

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

The suites use RSA for key transport, rather than using Diffie-Hellman for key exchange. They hence do not have perfect forward secrecy. If an attacker first records a TLS session, and then manages to get the private keys, they could decrypt the session. The risk of such an attack is limited for OCPP.

However, it is generally recommended to phase out cipher suites that do not support perfect forward secrecy, as there are suites that support it are readily available.

Id	Requirement
SEC-0209	For OCPP, the suites above could for instance be replaced by: - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

As the update in cipher suites is not urgent, it could be combined with the migration to TLS 1.3. TLS 1.3 requires the use of algorithms with perfect forward secrecy.

The elliptic curve cipher suites in OCPP 2.0.1 and 2.1 do support perfect forward secrecy. They are still recommended for long term use and there is no need to phase them out. For this reason:

Id	Requirement
SEC-0210	it is RECOMMENDED to use the elliptic curve suites over the RSA suites in the short term if possible.

7.1.3. Post-quantum cryptography

OCPP should be prepared for attack using quantum computers by implementing post-quantum cryptographic algorithms. Post-quantum algorithms are being standardized and are available in TLS.

Most governments present timelines for moving to post-quantum cryptography between 2030 and 2035. Charging stations do not have to be early adopters of post-quantum cryptography. They are not that vulnerable to “harvest now, decrypt later” attacks, where an attacker captures traffic now and then decrypts it when quantum computers become available. Hence, OCPP can wait with migrating to post-quantum algorithms until around 2035. Some countries may however put in place regulations that require CPOs to move to post-quantum cryptography sooner, especially if they are considered a critical infrastructure.

As Charging Stations are in the field for a long time, it is useful to start preparing OCPP and define a post-quantum cryptography option in the coming years.

An important consideration is also that the keys used for post-quantum algorithms are typically much larger. Charging stations that are installed now should at least have enough memory to support them (please refer to 12.4.6 for more details).

7.2. Managing backwards compatibility

Upcoming OCPP specification updates (errata & additions)

Implementing the updates discussed above can be challenging. Charging stations and CSMSs should be able to use the latest versions and features but should also be backwards compatible to allow connections with older equipment. It should however not be possible for attackers to exploit the backwards compatibility to downgrade to vulnerable TLS versions.

As a solution to meeting these conflicting objectives, the allowed TLS versions and cipher suites are bundled in *security policies*. The existing network connection profiles then provide a mechanism to control the security *profile*. The security *settings* - all settings related to TLS - that a Charging Station accepts can be managed by setting the `SecurityPolicy` via the device model.

The approach has two advantages:

- CPOs can enforce their own cryptographic policies on the Charging Stations, for instance to comply with national regulations on cryptography. By selecting a secure (or even custom) policy and avoiding unsecure security policies, as described below, the CPO can ensure that a Charging Station does not accept cryptographic algorithms that are not allowed by its policies. But if it is needed, they can allow older TLS version by configuring a different security policy on the Charging Station. The CPO hence can determine themselves their "risk appetite" for older TLS versions or cipher suites.
- The OCPP standard can define a long-term roadmap for upgrading TLS by uncoupling the relation between the TLS settings and the OCPP version. Policies for TLS 1.3 or with new cipher suites can already be defined for the current protocol versions (and explained / added via a whitepaper). The same versions can then be kept for future OCPP versions. For backwards compatibility reason, OCA defines a policy that captures the OCPP 2.0.1 / 2.1 security requirements that can be selected. In the future OCA can then gradually deprecate older security policies when they become vulnerable, first by recommending against their use, and then by deprecating and removing the policies in later versions.

7.2.1. Security profiles vs. security policies

Upcoming OCPP specification updates (errata & additions)

The basic idea is that each security profile in OCPP only describes the *mechanism* / *method* of security: basic authentication, TLS with basic authentication and TLS with client-side certificates. The TLS *settings* that are allowed, in particular the allowed TLS versions and cipher suites are captured in security *policies* that can be referred to with a unique name.

Current versions of the OCPP specification capture these two types of information in security profiles which therefore need to be updated in a future version of OCPP. See for instance requirements A00.FR.313, A00.FR.318, A00.FR.319, and A00.FR.320 for the TLS with basic authentication profile for requirements that would then not be specified anymore by these requirements, but separately in security policies.

Policies would be given a name of the form “OCPP-TLS<description>-<year>”, for instance OCPP-TLS12-

2020 or OCPP-TLS13-2025. Policies do not have to be ordered, as it is not always possible to say that one policy is strictly more secure than another.

7.2.2. Process for connecting

A Charging Station can then enforce the TLS settings by checking against the security policy in the device model when it connects to a CSMS. The Charging Station first sets up a TLS connection to the CSMS. The TLS version and cipher suites are negotiated during the TLS handshake. The Charging Station can then either adapt its options during TLS negotiation based on its active security policy or check if the negotiated settings are allowed by the security policy and, if they are not, close the connection (less error prone).

If a connection is not allowed and a fallback and / or other network connection profile is present on the Charging Station, the Charging Station will try these next.

7.2.3. Process for changing policies

The CSMS can update a Security policy by changing the relevant variable in the device model. Immediately after the change, the Charging Station will try to reconnect with the new policy. If the Charging Station fails to connect with the new policy, it will fall back to the old policy and send SecurityEventNotification `SecurityPolicyUpdateFailed`. Once successfully connected with the newly set policy the Charging Station will send a SecurityEventNotification `SecurityPolicyUpdated` and cannot fall back to the previous security policy. This can only be initiated by changing the security policy by the CSMS again.

On its side, the CSMS also checks the TLS settings against the security policies it has configured in the Charging Station. In most cases, the CSMS will support one security profile – security policy combination on a specific network address and port. The security profile and policy used would be an internal configuration of the CSMS.

To secure changing the security policy of a Charging Station, an additional security mechanism is needed to make sure that restoring a (less secure) security policy is not easily done. This topic is separately covered in chapter 9.

7.3. OCPP additions to the Device Model

Upcoming OCPP specification updates (errata & additions)

The proposed implementation of security policies is by adding 2 Device Model variables detailed in Appendix B. Reason for choosing these 2 variables instead of making it part of a NetworkConnectionProfile is that this makes it possible to apply this approach – for example based on a description in a whitepaper – to OCPP 2.0.1 and OCPP 2.1 without having to change the JSON schemas. The approach consists of an additional variable of type OptionList that contains a value from the list of supported security policies. The (actual) value can then be set to the policy that must be used.

To change security policy, the variable `SecurityPolicy` can be set to a new Security Policy that is to be used the next time the Charging Station reconnects to a CSMS. The variableInstance can be used to indicate the scope of the security policy: if the Charging Station does not have the variableInstance defined, the security policy applies to all security connections, otherwise a variableInstance is needed to specify the scope: *CSMSWebSocketConnection*, *FirmwareDownload* or *LogfileUpload*.

Besides the SecurityPolicies defined by OCA, implementers can add custom security policies (and variableInstances) depending on their own needs, for example when regulatory requirements ask for security policies that differ from the predefined policies[16]. SecurityPolicies defined by OCA will start with "*OCPP-*". Custom SecurityPolicies defined by a vendor SHALL start with a value that uniquely identifies the policy. It MUST be formed from the reversed DNS namespace, where the top tiers of the name, when reversed, should correspond to the publicly registered primary DNS name of the Vendor organization. For example: "*com.mycompany-POLICY123*".
This is the same naming rule as used for the vendorId in DataTransfer or CustomData customizations.

As the CSMS websocket connection is in use, a second variable - `ActiveCSMSSecurityPolicy` – is included to indicate the security policy the station uses at that moment to connect to the CSMS. When updating the security policy, it will temporarily have a different value than the `ActiveCSMSSecurityPolicy`.

8. Securing other services

OCA recommendations beyond OCPP

Besides OCPP, Charging Stations also use many other network protocols. They may use NTP for time synchronization, DNS for translating domain names to IP addresses, and FTP for file transfers.

Id	Requirement
SEC-0211	For the Charging Station to be secure, all network services (eg. NTP, DNS, FTP, …) MUST be secured.

The following paragraphs provide an overview what a vendor can do to secure these other services.

8.1. General security requirements

The following general security requirements apply for securing other services:

Id	Requirement
SEC-0212	To ensure a secure OCPP implementation, other network services MUST be secured, as indicated by legislation such as the RED delegated act, and on the ElaadNL / ENCS requirements.
SEC-0213	The services SHOULD use encryption, message authentication, and protection against replay attacks.

For many services, these properties can be provided by using TLS. In that case, the protocols can follow the OCPP requirements on the TLS configuration and cipher suites.

Other services may however use protocol-specific security measures. The OCPP security guidelines cannot cover all possible protocols. So, it should recommend following the best practices available for each protocol.

8.2. Protocol configuration

For the use of TLS in protocols, the following requirement applies:

Id	Requirement
SEC-0214	When protocols use TLS, they SHALL follow the security policy configured for TLS in OCPP (see 7).

Most other settings will however be protocol specific. OCPP can probably only support configuring the most used protocols. Recommendations for some are given below.

8.2.1. FTP configuration

One commonly used protocol is FTP, which the Charging Station uses to download firmware files or upload logs.

Id	Requirement
SEC-0215	It would be recommended to use FTPS to secure the FTP connection, as in that case TLS can be used. Using SFTP would also provide a secure connection but would use SSH keys which would have to be managed separately.

If the FTP server is integrated with the CSMS servers, it can use the CSMS authentication mechanisms. The FTP server could use a certificate in the Charging Station Operator hierarchy, so that the Charging Station can validate it using the CSMS root certificate. The Charging Station can use either client-side certificates (profile 3) or the basic authentication password (profile 2). If the basic authentication password is used, the FTP server needs to be trusted by the CSMS, as it would have access to the passwords. If it is not trusted, a separate FTP password needs to be configured.

Id	Requirement
SEC-0216	It is RECOMMENDED to use HTTPS instead of FTPS whenever possible, as HTTPS exposes a smaller attack surface.

8.2.2. HTTP

Charging Stations also use HTTP for other purposes than for the OCPP connection. They may, for instance, use it instead of FTP to download firmware or upload log files.

Id	Requirement
SEC-0217	Charging Stations MUST always use HTTPS instead of plain HTTP for security. The OCPP Security policies SHALL be followed for the TLS settings (see 7).

Certificate management depends on the use case. If the HTTP connections are to servers in the CSMS, the server certificates can be in the Charging Station Operator hierarchy that is used in OCPP for the CSMS. But for other use cases a separate certificate hierarchy could be needed. See the comments on certificate management below.

8.2.3. Network Time Security (NTS)

Since classical NTP can be easily manipulated, e.g., by introducing a fake time server, usage of NTS is highly recommended:

Id	Requirement
SEC-0218	For secure time synchronization it is RECOMMENDED to use TLS. As NTS uses TLS for security, it can also follow the OCPP Security Policies (see 7).

This requires direct communication between a Charging Station / local controller and the official NTS servers distributing legal time. As some CPOs do not allow secondary internet traffic bypassing their backend, NAT/masquerading has proven a useful alternative: The CPO backend reroutes NTS/NTP packets to the legal NTS server.

It has to be noted that port 123 is usually subject to rate limiting which must be reconfigured to allow for simultaneous usage by multiple NTP clients. To enable CPOs to automatically configure their clients,

a JSON configuration file might be made available by the national legal time server operators.
Upon first use of an NTS certificate installed in a Charging Station or local controller - especially if commissioning occurs much later than placing on the market - it is highly recommended to manually check the clock of the Charging Station or local controller to ensure correctness of the time source.

For managing the CA certificates, the certificate management use cases described below can be used. For the configuration, the Charging Station only needs the server address and a variable to turn on NTS.

8.2.4. DNS

In many cases, Charging Stations use DNS to resolve the address to connect to the CSMS. DNS is vulnerable to various attacks, such as spoofing and cache poisoning. For this reason:

Id	Requirement
SEC-0219	It is RECOMMENDED to use DNSSEC whenever possible.

The use of TLS does provide an authentication mechanism of the CSMS separate from DNS that mitigates some of the risks if properly implemented. If an attacker manages to point a Charging Station to the wrong IP address through DNS attacks, the Charging Station can detect that the host is not the CSMS by checking the certificate. Such attacks can however cause a denial-of-service.

8.2.5. SSH

Some Charging Stations use SSH for remote access. The SSH protocol in itself is secure, provided that the host key is trusted, see 3.4. However, it does pose a security risk because of the unrestricted access that it gives users, especially if they can have root privileges. With such privileges, users may for instance change executables and scripts, bypassing measures to protect firmware integrity. For this reason:

Id	Requirement
SEC-0220	SSH access MUST be used with caution.

It is probably easier to manage the SSH settings through SSH itself rather than through OCPP. Through SSH, users already have good options to manage user accounts and credentials. Adding such functions in OCPP is more complex.

It also could create additional risks as OCPP does not have separation of roles, which is available in SSH. To manage SSH setting, the CSMS would have to be given rights that are equivalent to root access. They may for instance create new SSH accounts and change their credentials. Attackers could abuse such functions to give themselves root access.

8.3. Certificate management

Upcoming OCPP specification updates (errata & additions)

Protocols that use certificates could use the existing OCPP certificate management use cases for their own certificates.

OCPP already includes several certificate management use cases:

- Updating CA certificates (M05)
- Updating the certificate of the Charging Station:
  - Using a Certificate Signing Request on request of the CSMS (A02)
  - Using a Certificate Signing Request on request of the Charging Station (A03)
- Deleting certificates (M04)
- Retrieving a list of available certificates (M03)

These use cases should be enough to support certificate management for most protocols. Certificates for different uses are now identified through the InstallCertificateUse enum type. This enum could be extended to cover other commonly used services, such as NTS and FTPS. If using an enum is too restrictive, a string identifier could be used in a future version of OCPP.

8.4. Using DANE

An alternative to setting up certificate management in OCPP, would be to use DNS-based Authentication of Named Entities (DANE). However:

Id	Requirement
SEC-0221	It is NOT RECOMMENDED to use DANE.

When using DANE, the Charging Station uses DNS to check if a certificate is valid, rather than using a CA certificate and certificate chain. The advantage of this approach is that no management is required for root certificates. As OCPP already has use cases to manage root certificate, this advantage however is limited. The disadvantage would be that the CPO would have to use DNSSEC, as the security of services now relies on DNS. Additionally, DANE does not seem to be widely used, so it is not clear if it can be easily implemented by Charging Station manufacturers.

For the above reasons, DANE is not recommended for OCPP deployments.

8.5. Security events for certificate management

Security events exist for any changes to certificates or keys. These events are now part of the ReconfigurationOfSecurityParameters event. It would be better to use separate events for changes to CA certificates and to private keys. These SecurityEvents will be added to a future version of the appendices of OCPP Part 2. Charging Station will be allowed (and even RECOMMENDED) to report these in addition to the ReconfigurationOfSecurityParameters event.

Security event	Description	Critical
CA certificate installed	A new CA certificate has been installed on the Charging Station (e.g. through use case M05). The tech info field of the security event notification request should contain the certificate use (as in the InstallCertificateUse enum type)	Yes

Security event	Description	Critical
Charging station certificate updated	A certificate and private key used for the identification of the Charging Station has been updated (e.g. through use cases A02 or A03).	Yes

The Charging Station certificate update event could be used for any certificate used to identify the Charging Station, also if the certificate is used for other protocols. In that case, the tech info field should also contain the certificate use.

Id	Requirement
SEC-0222	German law requires a log entry in a metrological log if the Root CA certificate for NTS is changed (see [PTB851]).

9. Restricting access to critical operations

Upcoming OCPP specification updates (errata & additions)

OCPP currently does not provide a method to restrict access to privileged functions on a Charging Station. After authentication, the CSMS has access to all functions on the Charging Station. There is no separation of roles that would allow to implement the principle of least privileges.
There are however some privileged functions where it would be useful to restrict access, such as:

- Updating CA certificates
- Performing firmware updates
- Performing financial transactions
- Switching power at many Charging Stations at the same time

The lack of role separation is made worse by the use of authorized man-in-the-middle (MitM) solutions used by some CPOs. Some CPOs for instance, route traffic to the CSMS through the servers of a third party to make use of their services. Other CPOs may use a local controller or an EMS as man-in-the-middle. The problem is that any system that is put in the middle will have the same access rights as the CSMS. So, it also has full access to all the privileged functions, which is usually not desirable.
In this chapter, we explore possible solutions to restrict access to these functions.

9.1. Possible solutions

The table below summarizes the possible solutions for restricting access to privileged functions with their advantages and disadvantages.

Solution	**Advantages**	**Disadvantages**
RBAC in the CSMS GUI	- Easy to implement - Protects against insider threats - Protects against attacks through compromised GUI accounts	- Does not protect in MitM scenario - No protection if attackers fully control the CSMS
Logging access to privileged functions	- Allows to analyze security incidents	- Does not protect in MitM scenario - Attackers that control CSMS can suppress event collection
Changes through firmware updates	- Would protect against attackers that fully control the CSMS	- CPO can only make changes with the help of the Charging Station manufacturer
Signing messages with the CSMS private key	- No new keys need to be introduced	- Relatively complex to implement - Does not protect in MitM scenario - No protection if attackers fully control the CSMS, as they can use the CSMS private key

Solution	Advantages	Disadvantages
Signing messages with other keys	- Protects against attackers with full control of the CSMS	- Very complex to implement

9.1.1. RBAC in the CSMS GUI

While roles cannot be separated in the OCPP protocol, they can be separated in the graphical user interface (GUI) of the CSMS.

Id	Requirement
SEC-0223	Preferably, a role-based access control (RBAC) model is used with centrally managed, individual user accounts and privileges assigned to roles. Privileged actions SHOULD be limited to specialized administrator accounts that are only used by a small number of trusted personnel.
SEC-0224	Access to these roles SHOULD be protected through two-factor authentication.
SEC-0225	For very critical actions, the four-eyes principle SHOULD be enforced. See also Human users.

With modern development frameworks, the RBAC should be relatively easy to implement. Having RBAC in the GUI will provide good protection against insider threats or compromised accounts.

But the solution will not protect in MitM scenarios where someone has compromised a system put in the middle between the CSMS and Charging Station. It will also not protect against attackers that manage to gain full control over the CSMS, as these can simply bypass the GUI.

9.1.2. Logging access to privileged functions

For logging access to privileged functions the following applies:

Id	Requirement
SEC-0226	The Charging Station SHOULD log all access to privileged functions.

Access to security related privileged functions, such as updates of CA certificates or firmware updates, can be logged in the security log and pushed to the CSMS using security event notifications (use case A04). If privileged functions are not security related, they should be logged in other logs.

Id	Requirement
SEC-0227	The CPO should set up monitoring to analyze and respond to the logged events.

Logging privileged functions will allow CPOs to better analyze security incidents. But the OCPP security logging mechanism provides no protection in MitM scenarios or against attackers who have compromised the CSMS. All logs are sent through the CSMS. So, attackers could simply suppress the events.

If CPOs want to protect in these cases, they could consider gathering the security logs through a different channel. The Charging System could for instance send the log directly to a SIEM system using syslog.

9.1.3. Changes through firmware updates

Critical changes to the Charging Station can be included in the firmware updates. The firmware updates can be protected using the digital signature of the Charging Station manufacturer. So, even in a MitM scenario or when the CSMS is completely compromised, attackers cannot just send any firmware they want to the Charging Station. At worst, they can downgrade firmware to an older version (if the Charging Station allows older version).

The downside of making changes to the firmware is that these can only be made with the help of the Charging Station manufacturer. Usually, the CPO should not be dependent on the manufacturer to change the configuration of their Charging Station, as the manufacturer may not support the Charging Station through its entire lifecycle.

9.1.4. Signing messages with the CSMS private key

Privileged actions could also be protected by using signed messages, as defined in Section 7 of OCPP 2.1 Part 4 - JSON over WebSockets implementation guide. The easiest way to do this would be to sign the messages using the CSMS private key that is also used for the TLS connection, as in that case no new keys need to be introduced.

Even then, this approach does add complexity. It should be defined which actions are privileged and may only be accessed using signed messages. Possibly, there would be a need to turn the protection through signing on and off. Error handling needs to be defined in case the signature is not correct. And if the CSMS uses an HSM to protect the keys, it could take some integration work to have the HSM sign the OCPP messages.

Additionally, this solution does not really protect in MitM scenarios or against attackers who have compromised the CSMS. In the MitM case, the system that is in the middle needs access to the CSMS private keys to function. So, if it is compromised, the system can also create signed messages. If the CSMS is compromised, we should assume that the attackers also have the CSMS private key. Even if the private key is held in an Hardware Security Module (HSM) and they cannot extract it, they can still use it to create signed messages and access the privileged functions.

9.1.5. Signing messages with other keys

To solve the problem with attackers gaining access to the CSMS private key, messages could be signed with other keys. A separate key could be introduced for specific privileged access such as key management of firmware updates. The private key could be kept outside the CSMS. So, even when attackers have compromised the CSMS, they cannot access the key to perform the privileged actions. Using a separate key would provide protection even in MitM scenarios or against attackers who have fully compromised the CSMS. But it would be a very complex solution. Besides the complexities when using the CSMS key discussed above, a new key hierarchy needs to be set up both at the CSMS and the Charging Station. The OCPP specification needs to define which key is used for which operation. CPOs need to store the keys in systems outside of the CSMS. But these outside systems still need to sign the OCPP messages.

9.2. Recommended solutions

Looking at the advantages and disadvantages, the following two solutions are RECOMMENDED for restricting access to critical functions:

Id	Requirement
SEC-0228	RBAC in the CSMS GUI SHOULD be used. Both the technical implementation in the CSMS and the account management processes at the CPO are needed to use RBAC effectively. See also Human users
SEC-0229	Logging all access to privileged functions in the security logs or other logs. In addition, monitoring MUST be used for critical functions. Please refer to OCPP 2.x specification Part 2 Appendices document for the available Security Events, such as `InvalidCsmsCertificate` and `TamperDetectionActivated` (see also 5.5.3). Besides setting up monitoring, the CPO MUST also respond to the logged events.

These above solutions are relatively easy to implement, and they provide good protection against most threats. However, the solutions do not provide protection in MitM scenarios or when attackers have fully compromised the CSMS. For these cases, the only real solution would be signing messages with other keys. Whether it is worth adding this measure to OCPP would mostly depend on how common the use of MitM solutions is. The threat of attackers fully taking over the CSMS can probably be mitigated more effectively by measures that protect the CSMS. But the risk caused by the use of MitM solutions would have to be addressed in the OCPP protocol itself.

Updating the root certificate

A special case of privileged functions is updates to CA certificates. OCPP allows the CSMS to install (M05) and delete (M04) CA certificates. Additional protection was included in OCPP 2.x in the form of an additional root certificate check:

Id	Requirement
SEC-0230	if the `AdditionalRootCertificateCheck` variable is set, the new root certificate MUST be signed using the old root certificate.

This way, the CSMS can only perform the update with authorization of the CA. An attacker would have to compromise both the CSMS and the CA to change the root CA. Currently an extension is added to also allow a new self-signed root by using a cross-signed rollover certificate.

The mechanism included in the additional root certificate check still seems a valid solution for this specific case. Cross-signing the new CA certificate with the old certificate is common practice for public CAs. It is also a commonly used measure in key management protocols such as SCEP or EST. So, it can be used to protect CA certificate updates in OCPP.

There are some availability risks in using the old CA certificate to cross sign the new CA certificate. If the private key of the old CA certificate would somehow be lost, it would not be possible to install a new CA certificate. Hence, it is critical to make a secure backup of this private key.

10. Local Controller security

Upcoming OCPP specification updates (errata & additions)

The security of Local Controllers is described in the Application Note "Local Controllers in OCPP 2.x" ([LC-2026]). As defined in this application note, a Local Controller (LC) is a concept from the OCPP 2.x specification that refers to a device that sits between the CSMS and any number of Charging Stations, creating a local group or cluster. The Local Controller acts as a Charging Station to the CSMS and as a CSMS to the Charging Station. It can then act as a man-in-the-middle for all communications between the CSMS and Charging Station.

A Local Controller acts as a proxy between a Charging Station and a CSMS. Typical for the "classic" Local Controller is, that it replicates every websocket connection it has to a Charging Station towards CSMS using the identity of the Charging Station. The Local Controller has its own websocket connection towards CSMS using its own identity.

As explained in the Application Note the following requirements apply for a secure implementation:

Id	Requirement
SEC-0231	Each Charging Station SHALL be paired to a unique Local Controller, so that other Local Controllers cannot connect to it. This is done by using a unique address for the Local Controller in its certificate.
SEC-0232	The Local Controller SHALL be managed remotely to receive security updates and periodic changes in credentials. A topology where the Local Controller does not have its own connection to a central system (such as the CSMS) SHALL NOT be used because this creates unacceptable risks.
SEC-0233	To set up a secure chain of CSMS, Local Controller and Charging Station(s), the security model from [LC-2026] for using Security Profile 2 or Security Profile 3 and key management requirements MUST be followed.
SEC-0234	In order to allow Charging Stations to connect to the Local Controller when the CSMS connection is offline, the Local Controller can keep a local (encrypted) file of Charging Station passwords. For this, the requirements for Charging Stations from 4.9 SHALL also be applied to the Local Controller.
SEC-0235	In order to allow Charging Stations to connect to the Local Controller when the CSMS connection is offline, the Local Controller can hold credentials in memory. Even in volatile memory, the credentials MUST still be treated as sensitive: avoid unnecessary copies, clear them when no longer needed where feasible, and protect logs/crash dumps from exposing them.
SEC-0236	The requirements for Charging Stations from 4.6 SHALL also be applied to the Local Controller.
SEC-0237	In specific circumstances an offline Local Controller is allowed to accept the connection of a Charging Station that is not yet authenticated and keep the Charging Station in a `Pending` state. The Local Controller SHALL make sure that the Charging Station cannot perform any actions in this `Pending` state.

SEC-0238	When a Local Controller requests a server certificate to connect to its Charging Stations using a process similar to updating Charging Station certificates (by sending a SignCertificateRequest for a new certificate type LCCertificate), the server certificate would be signed by the CSMS CA but it MUST include a unique identifier of the Local Controller in for instance the DNS-ID. Local controllers MUST not all use the same DNS name (such as “controller.local”) to avoid the risk that someone extracts a private key from one controller and uses it to connect to Charging Stations of other controllers.

11. Referenced documents

Ref.	Document	Version	Date	Link
[CCPA]	California Consumer Privacy Act (CCPA)	March 13 2024	2024-03-13	https://oag.ca.gov/privacy/ccpa
[CMMC]	Cybersecurity Maturity Model Certification (CMMC)	-	-	https://dodcio.defense.gov/CMMC/
[CRA]	Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)	2024-11-20	2024-11-20	https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
[CRACAT]	Commission Implementing Regulation (EU) 2025/2392 of 28 November 2025 on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council	2025-11-28	2025-11-28	https://eur-lex.europa.eu/eli/reg_impl/2025/2392/oj/eng
[CRA-GD]	C(2026) 5252 - Annex - Commission guidance on the application of the Cyber Resilience Act (CRA)	2026-07-26	2026-07-26	https://digital-strategy.ec.europa.eu/en/library/commission-publishes-new-guidance-support-timely-cyber-resilience-act-implementation
[DCPM]	Decreto del presidente del consiglio dei ministri 14 aprile 2021, n.81. Allegato B	-	2021-04-14	https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/SG
[EV-211]	Security requirements from IEC 62443 for EV charging infrastructure	2025v1.0	2025-02-25	https://encs.eu/resource/ev-211-security-requirements-from-iec-62443-for-ev-charging-infrastructure/

Ref.	Document	Version	Date	Link
[EV-311]	Security requirements from IEC 62443 for procuring EV charging stations	2025v1.0	2025-02-25	https://encs.eu/resource/ev-311-security-requirements-from-iec-62443-for-procuring-ev-charging-stations/
[EV-312]	EV-312: Implementing IEC 62443-4-2 requirements in OCPP 2.0.1 2025v1.0	2025v1.0	2025-02-25	https://encs.eu/resource/ev-312-implementing-iec-62443-4-2-requirements-in-ocpp-2-0-1/
[EV-313]	EV-313: Coverage of EN 18031 requirements by the IEC 62443 requirements for EV charging stations	1.0	2025-04-09	https://encs.eu/resource/ev-313-coverage-of-en-18031-requiremetns-by-ev-311/
[EN_18031-1]	EN 18031-1: Common security requirements for radio equipment - Part 1: Internet connected radio equipment	2024	2024-08-01	https://www.nen.nl/nen-en-18031-1-2024-en-328074
[EN_18031-2]	EN 18031-2: Common security requirements for radio equipment - Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment	2024	2024-08-01	https://www.nen.nl/nen-en-18031-2-2024-en-328073
[EN_18031-3]	EN 18031-3: Common security requirements for radio equipment - Part 3: Internet connected radio equipment processing virtual money or monetary value	2024	2024-08-01	https://www.nen.nl/nen-en-18031-3-2024-en-328072
[ENTSO-E]	Provisional Electricity Cybersecurity Impact Index by ENTSO for Electricity in cooperation with the EU DSO entity in accordance with Article 48 (2) of the Commission Regulation (EU) 2024/1366 of 11 March 2024 establishing a network code for cybersecurity aspects of cross-border electricity flows (ECII), ENTSO-E			https://eepublicdownloads.blob.core.windows.net/public-cdn-container/clean-documents/Network%20codes%20documents/NCCS/Provisional%20ECII.pdf

Ref.	Document	Version	Date	Link
[FSR]	Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique	-	2018-05-23	https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037444012
[MID-1]	DIRECTIVE 2014/32/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments (recast)	29.3.2014	2015-01-27	https://eur-lex.europa.eu/eli/dir/2014/32/oj/eng
[MID-2]	Commission Proposal for Targeted Amendment of the MID Adopted by the College of Commissioners	-	2024-11-29	https://single-market-economy.ec.europa.eu/document/dbca473a-69b7-49d6-89b3-44a52dd35fc6_en
[MID-3]	Directive (EU) 2026/706 Commission Proposal for Targeted Amendment of the MID Adopted by the College of Commissioners	-	2026-03-20	https://eur-lex.europa.eu/eli/dir/2026/706/oj/eng
[NCCS]	Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows	24.5.2024	2024-05-24	https://eur-lex.europa.eu/eli/reg_del/2024/1366/oj/eng
[NIS-2]	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)	2022-12-27	2022-12-27	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555
[ENT-SIZES]	Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises	2003-05-06	2003-05-20	https://eur-lex.europa.eu/eli/reco/2003/361/oj/eng

Ref.	Document	Version	Date	Link
[NIST]	NIST Handbook 44	2025	2025-01-10	https://www.nist.gov/pml/owm/nist-handbook-44-current-edition
[NIST-SP]	NIST SP 800-63B-4, Digital Identity Guidelines: Authentication and Authenticator Management, National Institute of Standards and Technology (NIST)	July 2025	-	https://doi.org/10.6028/NIST.SP.800-63B-4
[OIML]	OIML G 22 for Electric Vehicle Supply Equipment (EVSE)	Edition 2022 (E)	2022	https://www.oiml.org/en/publications/guides/en/files/pdf_g/g022-e22.pdf
[PTB851]	PTB-8.51-MB09-ZS-DE-V09, “Merkblatt: Zeitführung für Messgeräte, Zeitserver und Zeitserverinfrastrukturen”, Section 2.2 “Authentifiziertes NTP mittels NTS”, last revision 2 December 2025	-	2025	https://www.ptb.de/cms/fileadmin/internet/fachabteilungen/abteilung_8/8.5_metrologische_informationstechnik/8.51/PTB-8.51-MB09-ZS-EN-V09.pdf
[SNSS]	Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad	-	2022-05-04	https://www.boe.es/eli/es/rd/2022/05/03/311/con
[RFC5246]	T. Dierks, E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", August 2008	-	2008	https://datatracker.ietf.org/doc/html/rfc5246
[RFC7919]	D. Gillmor, "Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)", August 2016	-	2016	https://datatracker.ietf.org/doc/rfc7919/
[RFC8422]	Y. Nir, S. Josefsson, M. Pegourie-Gonnard, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier"	-	2016	https://datatracker.ietf.org/doc/rfc8422/
[RFC9116]	Foudil E., Shafranovich Y., "A File Format to Aid in Security Vulnerability Disclosure", RFC 9116, April 2022.	-	2022	https://www.ietf.org/rfc/rfc9116.txt
[RFC9525]	Saint-Andre P., Salz R., "Service Identity in TLS", RFC 9525, November 2023.	-	2023	https://www.ietf.org/rfc/rfc9525.txt

Ref.	Document	Version	Date	Link
[STAR-1]	Information-technology Promotion Agency, Japan (IPA), "Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements (JC-STAR) STAR-1 Conformance Requirements and Assessment Methods"	-	2024	https://www.ipa.go.jp/en/security/jc-star/tekigou-kizyun-guide/label1/s6ckaf000000ggej-att/STAR-1_Conformance_Requirements_and_Assessment_Methods.pdf
[LC-2026]	Open Charge Alliance, "Application Note: Local Controllers in OCPP 2.x"	-	2026	Link: to be published
[WP-16SEC]	Open Charge Alliance, Improved security for OCPP 1.6-J (a.k.a. OCPP 1.6 Security Whitepaper)	Edition 4	2026-02-05	Link: https://openchargealliance.org/my-oca/ocpp/
[OCPP-201]	Open Charge Alliance, OCPP 2.0.1 specification	Edition 4	2025-12-03	Link: https://openchargealliance.org/my-oca/ocpp/
[OCPP-21]	Open Charge Alliance, OCPP 2.1 specification	Edition 2	2025-12-03	Link: https://openchargealliance.org/my-oca/ocpp/

12. APPENDIX A: Security policies for OCPP

Upcoming OCPP specification updates (errata & additions)

OCPP uses TLS for setting up secure connections. To avoid vulnerabilities in the use of TLS, OCPP includes requirements and recommendations on TLS settings. These requirements and recommendations are up until OCPP version 2.1 mostly part of the security profiles.

In the future, the TLS settings will need to be updated, for instance to migrate to TLS version 1.3 or to post-quantum algorithms. To allow smooth updates, the TLS settings are decoupled from the security profiles. The TLS settings are in policies that can be controlled separately from the authentication profile using a variable in the device model.

To allow the decoupling, this appendix / document defines four Security policies for OCPP:

- OCPP-TLS12-2020 is mostly the same as the Security policy used in OCPP 2.1 and based on TLS version 1.2 with some minor changes based on discussions in the OCA Cyber Security Task Group. The changes are included as recommendations to preserve backwards compatibility with OCPP 2.1.
- OCPP-TLS12-2025: this policy is the same as OCPP-TLS12-2020 but all recommendations have been made mandatory.
- OCPP-TLS13-2025 is a new policy with settings based on TLS 1.3.
- OCPP-PQC-2026 is a new policy for Post-Quantum Crytography

12.1. OCPP-TLS12-2020

The OCPP-TLS12-2020 policy gathers the existing requirements in OCPP 2.1. These requirements are marked by the requirement number in front of them.

New recommendations have been added based on current best practices for TLS. The new recommendations are not made binding to keep compatibility with the OCPP 2.1 standard.

12.1.1. General

[A00.FR.050] For all cryptographic operations, only the algorithms recommended by ENISA in [1], which are suitable for use in future systems, SHALL be used. This restriction includes the signing of certificates in the certificate hierarchy.

[New] For all cryptographic operations, only the algorithms recommended by the European Cybersecurity Certification Group in [2] SHOULD be used. This restriction includes the signing of certificates in the certificate hierarchy.

12.1.2. TLS version

[A00.FR.313] The Charging Station and CSMS SHALL only use TLS v1.2 or above (see OCPP requirement A00.FR.313).

[A00.FR.314] Both of these endpoints SHALL check the version of TLS used.

[A00.FR.315] If either side detects that the other supports only older versions of TLS or SSL, it SHALL terminate the connection and trigger an InvalidTLSVersion security event.

12.1.3. Cipher suites

[A00.FR.318] The CSMS SHALL support at least the following four cipher suites:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

[A00.FR.319] The Charging Station SHALL support at least the cipher suites (see OCPP requirement A00.FR.319):

- (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 AND TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384) OR
- (TLS_RSA_WITH_AES_128_GCM_SHA256 AND TLS_RSA_WITH_AES_256_GCM_SHA384)

[New] The CSMS SHOULD support the following two cipher suites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

[New] The Charging Station SHOULD support at least the cipher suites (see OCPP requirement A00.FR.319):

- (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 AND TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384) OR
- (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 AND TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)

[A00.FR.320] The Charging Station and CSMS SHALL NOT use cipher suites that use cryptographic primitives marked as unsuitable for legacy use in [1]. This will mean that when one (or more) of the cipher suites described in this specification becomes marked as unsuitable for legacy use, it SHALL NOT be used anymore.

[A00.FR.322 / 323] If the Charging Station or CSMS detects that the other side of the connection only supports one of these legacy suites, it SHALL trigger an InvalidTLSCipherSuite security event AND terminate the connection.

[New] The Charging Station and CSMS SHOULD only use cipher suites that the BSI recommends for the period up to and including 2031 in [3].

[New] The Charging Station SHOULD use the extension "supported groups" ([RFC 7919] and [RFC 8422]) to inform the CSMS about the Diffie-Hellman groups it supports. The Charging Station SHOULD support at least one of the following Diffie-Hellman groups:

- secp256r1
- ffdhe3072

The CSMS SHOULD support both groups.

[New] The Charging Station SHOULD use the extension “signature_algorithms” ([RFC 5246]) to inform the CSMS about the signature algorithm it accepts. The Charging Station SHOULD support one of the following signature algorithms:

- rsa
- ecdsa

The CSMS SHOULD support both algorithms.

12.1.4. Certificates

[A00.FR.501] All certificates SHALL use a private key that provides security equivalent to a symmetric key of at least 112 bits according to Section 5.6.1 of [13]. This is the key size that NIST recommends for the period 2011-2030.

[A00.FR.502] For RSA or DSA, this translates into a key that SHALL be at least 2048 bits long.

[A00.FR.503] For elliptic curve methods, this translates into a key that SHALL be at least 224 bits long.

[A00.FR.505] For signing by the certificate authority RSA-PSS or ECDSA SHOULD be used.

[A00.FR.506] For computing hash values the SHA256 algorithm SHOULD be used.

[A00.FR.507] The certificates SHALL be stored and transmitted in the X.509 format encoded in Privacy-Enhanced Mail (PEM) format.

[A00.FR.508] All certificates SHALL include a serial number.

[A00.FR.509] The subject field of the certificate SHALL contain the organization name of the certificate owner in the O (organizationName) RDN.

[A00.FR.510] For the CSMS certificate, the subject field SHALL contain the FQDN of the endpoint of the server in the CN (commonName) RDN.

[New] For the CSMS certificate, the Subject Alternative Name (SAN) SHOULD include the DNS-ID identifier for the CSMS following RFC 9525. The Charging station SHOULD authenticate the server on the SAN DNS-ID if it is present. Only when the SAN field is not present in the certificate, SHOULD the Charging Station authenticate the server based on the CN.

[A00.FR.511] For the Charging Station certificate, the subject field SHALL contain a CN (commonName) RDN which consists of the unique serial number of the Charging Station. This serial number SHALL NOT be in the format of a URL or an IP address so that Charging Station certificates can be differentiated from CSMS certificates.

Note: According to RFC 2818, if a subjectAltName extension of type dnsName is present, that must be used as the identity. This would be incompliant with OCPP and ISO 15118. Therefore it SHOULD NOT be used in Charging Station. It is allowed to use the subjectAltName extension of type dnsName for a CSMS.

[A00.FR.512] For all certificates the X.509 Key Usage extension [5] SHOULD be used to restrict the usage of the certificate to the operations for which it will be used.

[A00.FR.513] If the Charging Station Certificate is also used as SECC Certificate in the ISO 15118 protocol, the certificate SHOULD also meet the requirements in ISO15118-2.

[A00.FR.514] For all certificates it is strongly RECOMMENDED NOT to use the X.509 Extended Key Usage extension, to be compatible with the ISO 15118 standard. There are alternative mechanisms available.

12.1.5. Other TLS settings

[A00.FR.321] The TLS Server and Client SHALL NOT use TLS compression methods to avoid compression side-channel attacks and to ensure interoperability as described in Section 6 of [10].

[New] Session renegotiation SHOULD only be allow on the basis of RFC 5746. The CSMS SHOULD reject renegotiation initiated by the Charging Station.

[New] The "truncated_hmac" extension in RFC 6066 SHOULD NOT be used.

[New] The TLS extension "encrypt-then-MAC" from RFC 7366 SHOULD be used.

[New] The Heartbeat extension specified in RFC 6520 SHOULD not be used to protect against the Heartbleed vulnerability.

[New] The Extended Master Secret extension defined in RFC 7627 SHOULD be used.

[New] Maximum Fragment Length Negotiation Extension, as specified in RFC 6066, SHOULD be supported.

[New] TLS session resumptions SHOULD be supported.

[New] The Charging Station and CSMS SHOULD support the Server Name Indication.

12.2. OCPP-TLS12-2025

The OCPP-TLS12-2025 policy is the same as OCPP-TLS12-2020, except that most recommendations have been made mandatory and the Extended Key Usage extension is now allowed.

12.2.1. General

[A00.FR.050] For all cryptographic operations, only the algorithms recommended by ENISA in [1], which are suitable for use in future systems, SHALL be used. This restriction includes the signing of certificates in the certificate hierarchy.

[New] For all cryptographic operations, only the algorithms recommended by the European Cybersecurity Certification Group in [2] SHALL be used. This restriction includes the signing of certificates in the certificate hierarchy.

12.2.2. TLS version

[A00.FR.313] The Charging Station and CSMS SHALL only use TLS v1.2 or above (see OCPP requirement A00.FR.313).

[A00.FR.314] Both of these endpoints SHALL check the version of TLS used.

[A00.FR.315] If either side detects that the other supports only older versions of TLS or SSL, it SHALL terminate the connection and trigger an InvalidTLSVersion security event.

12.2.3. Cipher suites

[A00.FR.318] The CSMS SHALL support at least the following four cipher suites:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

[New] The CSMS SHALL support the following two cipher suites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

[New] The Charging Station SHALL support at least the cipher suites (see OCPP requirement A00.FR.319):

- (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 AND TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384) OR
- (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 AND TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)

[A00.FR.320] The Charging Station and CSMS SHALL NOT use cipher suites that use cryptographic primitives marked as unsuitable for legacy use in [1]. This will mean that when one (or more) of the cipher suites described in this specification becomes marked as unsuitable for legacy use, it SHALL NOT be used anymore.

[A00.FR.322 / 323] If the Charging Station or CSMS detects that the other side of the connection only supports one of these legacy suites, it SHALL trigger an InvalidTLSCipherSuite security event AND terminate the connection.

[New] The Charging Station and CSMS SHALL only use cipher suites that the BSI recommends for the period up to and including 2031 in [3].

[New] The Charging Station SHALL use the extension "supported groups" ([RFC 7919] and [RFC 8422]) to inform the CSMS about the Diffie-Hellman groups it supports. The Charging Station SHALL support at least one of the following Diffie-Hellman groups:

- secp256r1
- ffdhe3072

The CSMS SHALL support both groups.

[New] The Charging Station SHALL use the extension “signature_algorithms” ([RFC 5246]) to inform the CSMS about the signature algorithm it accepts. The Charging Station SHALL support one of the following signature algorithms:

- rsa
- ecdsa

The CSMS SHALL support both algorithms.

12.2.4. Certificates

[A00.FR.501] All certificates SHALL use a private key that provides security equivalent to a symmetric key of at least 112 bits according to Section 5.6.1 of [13]. This is the key size that NIST recommends for the period 2011-2030.

[A00.FR.502] For RSA or DSA, this translates into a key that SHALL be at least 2048 bits long.

[A00.FR.503] For elliptic curve methods, this translates into a key that SHALL be at least 224 bits long.

[A00.FR.505] For signing by the certificate authority, RSA-PSS, ECDSA, or EdDSA SHOULD be used.

[A00.FR.506] For computing hash values the SHA256, SHA384 or SHA512 algorithms SHOULD be used.

[A00.FR.507] The certificates SHALL be stored and transmitted in the X.509 format encoded in Privacy-Enhanced Mail (PEM) format.

[A00.FR.508] All certificates SHALL include a serial number.

[A00.FR.509] The subject field of the certificate SHALL contain the organization name of the certificate owner in the O (organizationName) RDN.

[A00.FR.510] For the CSMS certificate, the subject field SHALL contain the FQDN of the endpoint of the server in the CN (commonName) RDN.

[New] The Charging station SHALL authenticate the server on the Subject Alternative Name (SAN) if it is present. Only when the SAN field is not present in the certificate, SHALL the Charging Station authenticate the server based on the CN. For the CSMS certificate, the SAN SHOULD include the DNS-ID identifier for the CSMS following RFC 9525.

[A00.FR.511] For the Charging Station certificate, the subject field SHALL contain a CN (commonName) RDN which consists of the unique serial number of the Charging Station. This serial number SHALL NOT be in the format of a URL or an IP address so that Charging Station certificates can be differentiated from CSMS certificates.

Note: According to RFC 2818, if a subjectAltName extension of type dnsName is present, that must be used as the identity. This would be incompliant with OCPP and ISO 15118. Therefore it SHOULD NOT be used in a Charging Station. It is allowed to use the subjectAltName extension of type dnsName for a CSMS.

[A00.FR.512] For all certificates the X.509 Key Usage extension [5] SHOULD be used to restrict the usage of the certificate to the operations for which it will be used.

[A00.FR.513] If the Charging Station Certificate is also used as SECC Certificate in the ISO 15118 protocol, the certificate SHOULD also meet the requirements in ISO15118-2.

[New] It is RECOMMENDED to use the X.509 Extended Key Usage extension, even though this extension is not used in the ISO 15118 standard. The CSMS certificate SHOULD have the serverAuth usage in its certificate. The Charging Station SHOULD have the clientAuth usage in its certificate, but SHOULD NOT have the serverAuth usage. Other usages SHOULD NOT be included in the certificates. The CSMS and Charging Station SHOULD check that the clientAuth and serverAuth usages respectively are included and SHOULD refuse the connection otherwise.

12.2.5. Other TLS settings

[A00.FR.321] The TLS Server and Client SHALL NOT use TLS compression methods to avoid compression side-channel attacks and to ensure interoperability as described in Section 6 of [10].

[New] Session renegotiation SHALL only be allow on the basis of RFC 5746. The CSMS SHALL reject renegotiation initiated by the Charging Station.

[New] The “truncated_hmac” extension in RFC 6066 SHALL NOT be used.

[New] The TLS extension “encrypt-then-MAC” from RFC 7366 SHALL be used.

[New] The Heartbeat extension specified in RFC 6520 SHALL not be used to protect against the Heartbleed vulnerability.

[New] The Extended Master Secret extension defined in RFC 7627 SHALL be used.

[New] Maximum Fragment Length Negotiation Extension, as specified in RFC 6066, SHALL be supported.

[New] TLS session resumptions SHALL be supported.

[New] The Charging Station and CSMS SHALL support the Server Name Indication.

12.3. OCPP-TLS13-2025

The OCPP-TLS13-2025 policy creates a policy to enforce the use of TLS version 1.3. The OCPP-TLS12-2025 policy does allow the use of TLS 1.3, however, the OCPP-TLS13-2025 policy *only* allows TLS 1.3 or newer and does *not* allow the use of TLS version 1.2.

TLS version 1.3 is designed to have fewer configuration options than version 1.2. Consequently, the OCPP-TLS13-2025 policy is shorter and simpler than the OCPP-TLS12-202x policies.

12.3.1. General

For all cryptographic operations, only the algorithms recommended by BSI in [12], which are suitable for use in future systems, SHALL be used. This restriction includes the signing of certificates in the certificate hierarchy.

12.3.2. TLS version

The Charging Station and CSMS SHALL only use TLS v1.3 or above (see OCPP requirement A00.FR.313).

Both of these endpoints SHALL check the version of TLS used.

If either side detects that the other supports only older versions of TLS or SSL, it SHALL terminate the connection and trigger an InvalidTLSVersion security event.

12.3.3. Cipher suites and other cryptographic algorithms

The CSMS and Charging Station SHALL both support at least the following two cipher suites:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384

The Charging Station and CSMS SHALL only use cipher suites that the BSI recommends for the period up to and including 2031 in [3].

The Charging Station SHALL support at least one of the following key exchange groups:

- secp256r1
- ffdhe3072

The CSMS SHALL support both above key exchange groups.

The Charging Station SHALL support at least one of the following signature algorithms:

- ecdsa_secp256r1_sha256
- rsa_pss_rsae_sha256
- rsa_pss_pss_sha256
- ed25519

The CSMS SHALL support all of the above signature algorithms.

12.3.4. Other TLS settings

To protect against the Heartbleed vulnerability, the Heartbeat extension specified in RFC 6520 SHALL NOT be used.

Please note that BSI indicates the following [3]: *"TLS 1.3 offers an option to include application data already in the first message of a PSK handshake (zero round-trip time data, abbreviated 0-RTT data). This data is not protected against replay attacks. Therefore, sending or accepting 0-RTT data is not recommended."*

12.4. OCPP-PQC-2026

The OCPP-PQC-2026 policy creates a policy for the use of post-quantum cryptography for the OCPP cryptographic functions, in particular the use of TLS and digital signatures.

The PQC policy should be considered as experimental, as not all recommended algorithms have been fully standardized within TLS through RFCs. Where possible, the policy uses algorithms that have been standardized by NIST in their Post-Quantum Cryptography Standardization program and are widely recognized by other governmental organizations such as BSI, ANSSI, and the European Cybersecurity Certification Group Sub-group on Cryptography. The only exception is the FALCON algorithm for digital signatures. This algorithm is still in a draft stage at NIST. It is included because it offers good performance for digital signatures on embedded systems.

While the algorithms are standardized, their integration into TLS is still in the IETF draft stage. The post-quantum key exchange and signature algorithms for TLS have not yet been published as RFCs.

12.4.1. General

For all cryptographic operations, only the algorithms recommended by BSI in [4] that are considered quantum-safe SHALL be used. This restriction includes the signing of certificates in the certificate hierarchy.

12.4.2. TLS version

The Charging Station and CSMS SHALL only use TLS v1.3 or above (see OCPP requirement A00.FR.313). Both endpoints SHALL check the version of TLS used. If either side detects that the other supports only older versions of TLS or SSL, it SHALL terminate the connection and trigger an InvalidTLSVersion security event.

12.4.3. Cipher suites and other cryptographic algorithms

The CSMS and Charging Station SHALL both support at least the following cipher suite:

- TLS13-AES256-GCM-SHA384

The Charging Station and CSMS SHALL only use cipher suites that the BSI recommends for the period up to and including 2031 and that are considered quantum-safe in [3].

The Charging Station SHALL support at least one of the following key exchange groups as defined in [6]:

- X25519MLKEM768
- SecP256r1MLKEM768
- SecP384r1MLKEM1024

The key exchange algorithms use a hybrid approach that combines a post-quantum algorithm with a classical elliptic curve algorithm. This approach is recommended as the quantum-safe algorithms are not yet as trusted as the classical algorithms (see [3] Section 2.2).

The CSMS SHALL support all above key exchange groups.

The Charging Station SHALL support at least one of the following signature algorithms as defined in [7] and [8]:

- mldsa65
- slhdsa_sha2_192s
- slhdsa_sha2_192f

The CSMS SHALL support all the above signature algorithms.

12.4.4. Firmware signatures

For validating the digital signature of firmware (requirement L01.FR.04 in OCPP 2.1), the Charging Station SHALL use a hybrid approach, combining a quantum-safe algorithm with an elliptic curve algorithm.

For the quantum-safe digital signature algorithm, the Charging Station SHALL use one of the following algorithms:

- mldsa65 or mldsa87 (CRYSTALS-Dilithium, see [9])
- slhdsa_sha2_192s slhdsa_sha2_192f, slhdsa_sha2_256s or slhdsa_sha2_256f (SPHINCS+, see [10])
- fndsa1024 (FALCON, see [11])

12.4.5. Other TLS settings

The Heartbeat extension specified in RFC 6520 SHALL not be used to protect against the Heartbleed vulnerability.

12.4.6. Certificate sizes when using Post-Quantum Algorithms

When using Post-Quantum algorithms, the public keys and signatures are significantly longer than with classical cryptography. As the life span of a Charging Station can be long, Charging Station manufacturers should already take this into account when designing and manufacturing Charging Stations.

The OCPP specification provides messages to exchange certificates and CSRs between the CSMS and the Charging Station. These messages follow the JSON schemas that include a maximum length for each field. The table below gives estimates for the size of a Certificate Signing Request (CSR) and certificate with the selected algorithms:

	mldsa65	slhdsa_sha2_192s	slhdsa_sha2_192f
Public key size	1,952 bytes	48 bytes	48 bytes

Signature size	3,309 bytes	16,224 bytes	35,664 bytes
CSR size	~ 5.5 KB	~16.5 KB	~36 KB
Certificate size	~ 6 KB	~17 KB	~36 KB

In OCPP 2.1 the SignCertificateRequest message has 5,500 characters for a PEM encoded CSR and the CertificateSignedRequest message has 10,000 characters for a PEM encoded certificate. As PEM encoding is Base64, it expands the sizes from the table above by 33%.

In future versions of OCPP these message lengths will be updated. When the message length is too small in the currently used version of OCPP, Charging Stations can still implement the OCPP messages with these larger certificates. A Charging Station can let the CSMS know it supports a higher field size by reporting this using the device model as:

```
OCPPCommCtrlr.FieldLength["<MessageName.FieldName>"] = <New max length>
```

For example, to extend the size of these messages to be used with the post-quantum algorithms with at least 50,000 to 60,000 bytes (perhaps more would be recommended to have some buffer), a Charging Station adds a variable to its Device Model as follows:

```
OCPPCommCtrlr.FieldLength["SignCertificateRequest.csr"] = 80,000
```

12.5. References

Ref.	Document	Date
[1]	ENISA European Network and Information Security Agency, „Algorithms, key size and parameters report 2014,"	2014
[2]	European Cybersecurity Certification Group Sub-group on Cryptography, „Agreed Cryptographic Mechanisms version 2.0	2025
[3]	Bundesamt für Sicherheit in der Informationstechnik, „Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths: Part 2 – Use of Transport Layer Security (TLS),"	2025
[4]	Federal Office for Information Security (BSI), „BSI TR-02102-1: Cryptographic Mechanisms: Recommendations and Key Lengths version 2026-01	2026
[5]	RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. https://www.ietf.org/rfc/rfc5280.txt	2008
[6]	K. Kwiatkowski, P. Kampanakis, B. Westerbaan and D. Stebila, „draft-ietf-tls-ecdhe-mlkem-04: Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3,"	2025
[7]	T. Hollebeek, S. Schmieg and B. Westerbaan, „draft-ietf-tls-mldsa-02: Use of ML-DSA in TLS 1.3,"	2026

Ref.	Document	Date
[8]	T. Reddy, T. Hollebeek, J. Gray and S. Fluhrer, „draft-reddy-tls-slhdsa-02: Use of SLH-DSA in TLS 1.3,"	2026
[9]	National Institute of Standards and Technology (NIST), „FIPS 204: Module-Lattice-Based Digital Signature Standard,"	2024
[10]	National Institute of Standards and Technology (NIST)," FIPS 205: Stateless Hash-Based Digital Signature Standard."	2024
[11]	P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte and Z. Zhang, „Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU,"	2020
[12]	Bundesamt für Sicherheit in der Informationstechnik: Anwendungshinweise und Interpretationen zum Schema, AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3.0, Bonn, Germany, May 2013. (in German) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_pdf.html	2013
[13]	National Institute of Standards and Technology. Special Publication 800-57 Part 1 Rev. 4, Recommendation for Key Management. January 2016. https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/final	2016

13. APPENDIX B: Device Model Variables

Upcoming OCPP specification updates (errata & additions)

13.1. SecurityCtrlr.SecurityPolicy

Required	No		
Component	**componentName**	SecurityCtrlr	
Variable	**variableName**	SecurityPolicy	
	variableInstance	Scope of the SecurityPolicy, one of: “CSMSWebSocketConnection”, “FirmwareDownload”, “LogfileUpload”.	
	variableAttributes	**mutability**	ReadWrite
	variableCharacteristics	**dataType**	OptionList
		valuesList	List of supported security policies, e.g. OCPP-TLS12-2020, OCPP-TLS12-2025, OCPP-TLS13-2025
Description	This Configuration Variable can be used to configure the security policy the station must use the next time it reconnects to a CSMS. implementers can choose from a number of predefined OCA security policies, but it is also allowed to add custom policies, for example if this is required by regulatory requirements.		

13.2. SecurityCtrlr.ActiveCSMSSecurityPolicy

Required	No		
Component	**componentName**	SecurityCtrlr	
Variable	**variableName**	ActiveCSMSSecurityPolicy	
	variableInstance	Scope of the SecurityPolicy, one of: “CSMSWebSocketConnection”, “FirmwareDownload”, “LogfileUpload”.	
	variableAttributes	**mutability**	ReadOnly
	variableCharacteristics	**dataType**	OptionList
		valuesList	List of supported security policies, e.g. OCPP-TLS12-2020, OCPP-TLS12-2025, OCPP-TLS13-2025
Description	Indicates the security policy the station uses at that moment to connect to the CSMS (so the instance “CSMSWebSocketConnection” of the `SecurityPolicy` variable).		

14. APPENDIX C: Overview of security issues found in Charging Stations

To give a sense of what type of vulnerabilities are currently present in Charging Stations, the following figure provides an overview of vulnerabilities found in 34 Charging Stations that have been tested for security by ElaadNL and that have published vulnerabilities based on participation in the Pwn2Own hackers competition (in 2024 and 2025). Please refer to the table below for the figure to the exact percentages and paragraphs in this document where guidance is provided for this type of vulnerability.

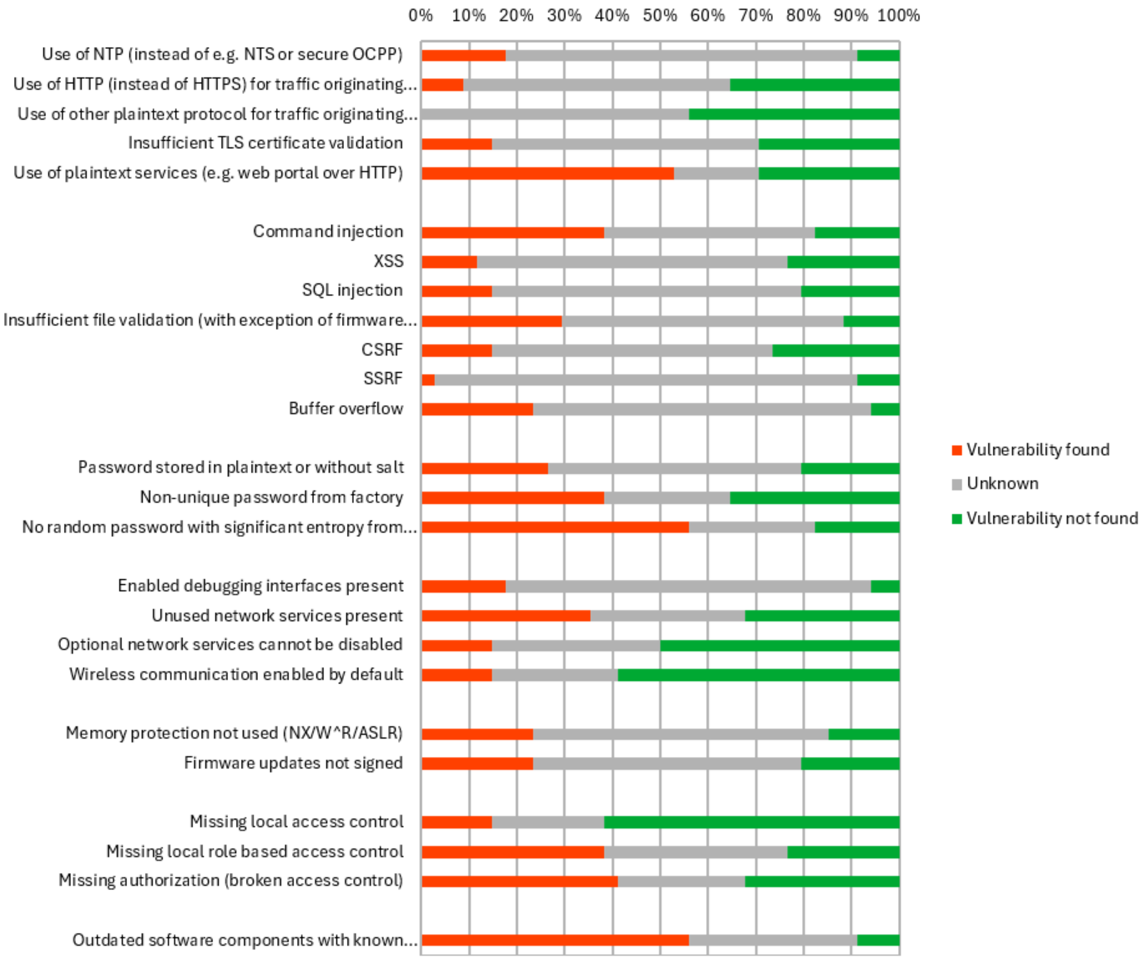

Figure 1. Overview of security vulnerabilities found in Charging Stations

In this figure and table, in case a vulnerability was found in a Charging Station, it is counted as "*Present*". If a thorough test was done for a vulnerability but it was not found, it is listed as "*Not present*". In case no testing was done for a vulnerability or if it is unknown whether it was tested for this vulnerability, it is counted as "*Unknown*"

Table 3. Overview of vulnerabilities found in Charging Stations

Vulnerability	Paragraph	Present	Not present	Unknown
Use of NTP (instead of NTS)	8.2.3	18%	9%	74%
Use of HTTP (instead of HTTPS) for traffic originating from charger	4.2, 3.4, 8.2.2, 4.12	9%	35%	56%

Vulnerability	Paragraph	Present	Not present	Unknown
Use of other plaintext protocol for traffic originating from charger	4.2, 8.2.2	0%	44%	56%
Insufficient TLS certificate validation	4.2	15%	29%	56%
Use of plaintext services (e.g. web portal over HTTP)	3.6, 8.2.2, 4.12	53%	29%	18%
Command injection	3.6	38%	18%	44%
XSS	3.6	12%	24%	65%
SQL injection	3.6	15%	21%	65%
Insufficient file validation (with exception of firmware signature check)	3.6	29%	12%	59%
CSRF	3.6	15%	26%	59%
SSRF	3.6	3%	9%	88%
Buffer overflow	3.6	24%	6%	71%
Password stored in plaintext or without salt	4.4.1	26%	21%	53%
Non-unique password from factory	4.6	38%	35%	26%
No random password with significant entropy from factory	4.6	56%	18%	26%
Enabled debugging interfaces present	4.9	18%	6%	76%
Unused network services present	4.12	35%	32%	32%
Optional network services cannot be disabled	4.12	15%	50%	35%
Wireless communication enabled by default	4.12	15%	59%	26%
Memory protection not used (NX/W^X/ASLR)	4.12	24%	15%	62%
Firmware updates not signed	4.8	24%	21%	56%
Missing local access control	4.13	15%	62%	24%
Missing local role based access control	4.13	38%	24%	38%
Missing authorization (broken access control)	4.6 and 4.2	41%	32%	26%
Outdated software components with known vulnerabilities	3.6 and 3.7	56%	9%	35%

[1] A harmonized standard is a European standard that is formally linked to specific EU legislation. By complying with the relevant harmonized standard, a product is generally presumed to meet the corresponding legal requirements of that legislation.

[2] Note: manufacturers choosing to build their own MID devices face additional regulatory requirements, particularly in jurisdictions like the EU.

[3] Both ENCS and ElaadNL are owned by the Dutch grid operators

[4] CIO - Cybersecurity Maturity Model Certification: https://dodcio.defense.gov/CMMC/Model/

[5] https://www.nist.gov/system/files/documents/2025/01/10/2025-HB-44-20250106-Final-508.pdf

[6] https://www.ipa.go.jp/en/security/jc-star/tekigou-kizyun-guide/label1/s6ckaf000000ggej-att/STAR-1_Conformance_Requirements_and_Assessment_Methods.pdf

[7] Encryption refers to transport or file encryption.

[8] Please note that this requires DNSSEC

[9] For OCPP 1.6 this is chapter 2 of the Security Whitepaper (officially titled: "*Improved security for OCPP 1.6-J*") ([WP-16SEC])

[10] Please note that similar privacy and security requirements exist under the GDPR, particularly through the concepts of data minimisation, pseudonymisation, security of processing, data protection by design and by default, and integrity and confidentiality.

[11] When using web portals, besides authentication, authorization is also important: functions must check whether a user is logged in.

[12] The JC-STAR defines constrained device as a device which has physical limitations in either the ability to process data, the ability to communicate data, the ability to store data or the ability to interact with the user, due to restrictions that arise from its intended use

[13] See: https://www.entsoe.eu/network_codes/nccs/ under “All TSO approved proposals for Methodologies.” At the time of writing, the methodology still needs to be approved by the competent authorities for the NCCS.

[14] This requirement is aligned with the EVCAN EVCMS Specification 1.1. For platforms using cloud services, EVCAN recognizes SOC 2, ISO/IEC 27017, FedRAMP, and CSA STAR as applicable security assurance frameworks. See https://www.evcan.org/ for more details.

[15] Please also note that using OCPP 2.x without TLS - i.e. without implementing Security Profile 2 (TLS with Basic Authentication) and optionally 3 (TLS with client-side certificates) - is only allowed during development and debugging and NOT for production

[16] It is highly recommended to only add custom policies that are equally or more secure than pre-defined policies (so at least TLS 1.2) to not introduce security vulnerabilities.