EV-301-2019

Security requirements for procuring EV charging stations

Version 2.0

24 December 2019

This document was produced by ElaadNL and ENCS as part of a program to improve the security of the electric vehicle charging infrastructure. The document is part of a series of requirements available through the ENCS portal (https://encs.eu/documents):

Smart metering	DA-301-2019: Security requirements for procuring smart meters and data concentrators
Distribution automation	DA-101-2019: Security risk assessment for distribution automation systems DA-201-2019: Security architecture for distribution automation systems DA-301-2019: Security requirements for procuring distribution automation RTUs DA-390-2019: Market survey on distribution automation RTU security DA-401-2019: Security test plan for distribution automation RTUs
Substation automation	DA-101-2019: Security risk assessment for substation automation systems DA-201-2019: Security architecture for substation automation systems DA-301-2019: Security requirements for procuring substation gateways DA-302-2019: Security requirements for procuring IEDs DA-303-2019: Security requirements for procuring HMI software
Electric vehicles	EV-101-2019: Security risk assessment for EC charging infrastructure EV-201-2019: Security architecture for EV charging infrastructure EV-301-2019: Security requirements for procuring EV charging stations EV-401-2019: Security test plan for EV charging stations

This document is shared under the Traffic Light Protocol classification:

TLP White – public

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

Version History

Date	Version	Description
4 April 2016	1.0	Initial release of requirements from Elaad Cyber-security project
7 August 2017	1.01	Requirements to authentication terminal simplified.
4 September 2019	1.9	Updated release from ENCS member project on procuring secure equipment.
16 September 2019	1.9.1	Minor changes after risk assessment: • Added measure PH3 on physical access to the local maintenance interface
22 October 2019	1.9.2	Minor updates to align with other requirements sets
5 November 2019	1.9.3	Minor updates after ENCS internal review
24 December 2019	2.0	Final version in ENCS member project on procuring secure equipment

ENCS

Table of Contents

Version History 3

1 Introduction 6

1.1 Scope 6

2 Access control 10

2.1 User access management [A.9.2] 10

2.2 System and application access control [A.9.3] 11

3 Cryptography 13

3.1 Cryptographic controls [A.10.1] 13

4 Physical and environmental security 15

4.1 Equipment [A.11.2] 15

5 Operations security 16

5.1 Operational procedures and responsibilities [A.12.1] 16

5.2 Backup [A.12.3] 16

5.3 Logging and monitoring [A.12.4] 17

5.4 Control of operational software [A.12.5] 18

5.5 Technical vulnerability management [A.12.6] 18

6 Communication security 20

6.1 Network security management [A.13.1] 20

7 System acquisition, development and maintenance 21

7.1 Security in development and support processes [A.14.2] 21

8 Supplier relationships 24

8.1 Information security in supplier relationships [A.15.2] 24

9 Information security aspects of business continuity management 25

9.1 Information security continuity [A.17.1] 25

Appendix A: Implementing the requirements in OCPP 2.0 26

Requirements fully covered by OCPP 2.0 26
Requirements partially covered by OCPP 2.0 26
Requirements not covered by OCPP 2.0 28
Glossary 29
References 30

1 Introduction

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

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

The cyber-attacks on Ukrainian grid operators [2] have shown that there are hackers that have the skills and motivation to disrupt the power grid. But this also means that CPOs are a target for cyber-attacks. If attackers gain control of a CPO's infrastructure, they could switch the power on the connected charging stations. Such an attack would not only hurt the CPOs themselves. The switching could also cause grid imbalances in the supply and demand for electricity and, possibly, power outages. If smart charging is used, attackers may force charging stations to use more power than assigned to them, which could damage transformers and power lines.

To mitigate these risks, grid operators as members of ENCS and ElaadNL have asked these organizations to develop a harmonized set of requirements that CPOs can use in their procurement documents for charging stations.

Harmonizing the requirements allows CPOs to get secure charging stations more cost-effectively: It should reduce time and effort in developing requirements, as they are already freely available. It ensures the requirements are feasible, as they have been tested in a market survey and in previous tenders by other operators. It also reduces implementation costs, because vendors get a common baseline from the clients to aim at and only need to implement the security requirements once.

Many of the requirements are already met if the charging station complies with the OCPP 2.0, as explained in Appendix A.

1.1 Scope

This document gives requirements for procuring remotely controlled charging stations. The architecture concerns the interfaces to the charging station and the users on these interfaces (see Figure 1). The architecture does not consider the internal working of the charging station.

The measures are aligned with ISO 27001:2013 [3] and cover the following sections from Annex A of that document:

- Access control (A.9)
- Cryptography (A.10)
- Physical and environmental security (A.11)
- Operations security (A.12)
- Communication security (A.13)
- System acquisition, development and maintenance (A.14)
- Supplier relationships (A15)
- Information security aspects of business continuity (A.17)

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

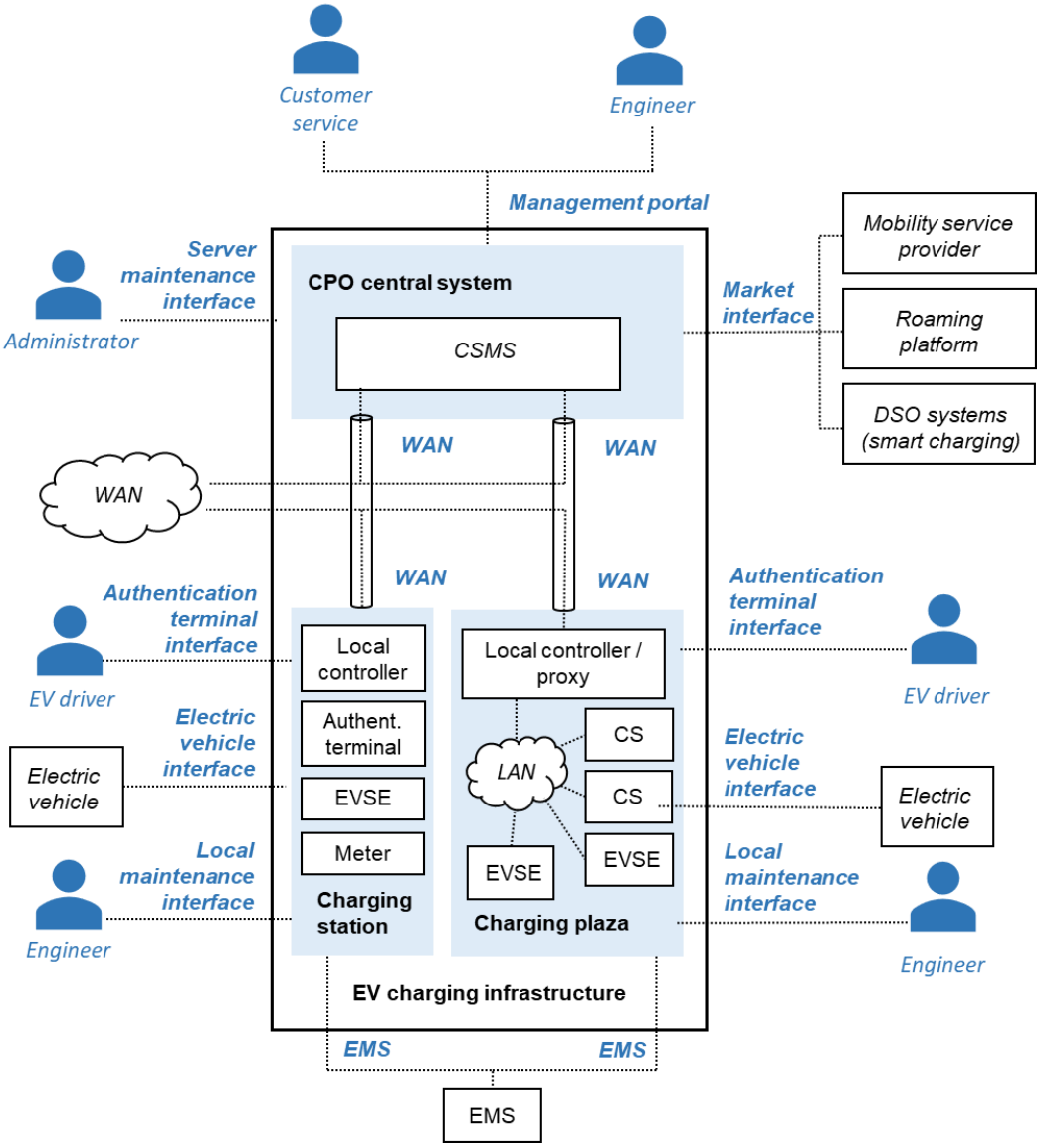

Figure 1: Reference architecture for the EV charging station, showing its users and interfaces.

Using the requirements

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

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

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

To ensure the quality of the processes and procedures, it is recommended to use an information security management system, for instance based on the ISO 27001 [3]. To support this, the architecture is organized by the security objectives in ISO 27001 [3] Annex A.

2 Access control

Access control requirements concern how access rights are managed and how strong the authentication needs to be for different user groups. The charging station supports access control for the user groups in Table 1.

Table 1: User groups on the charging station.

User	Required access	Interface
Charging Station Management System (CSMS)	• Gather information • Manage configuration • Update firmware	WAN
Engineer	• Manage configuration • Update firmware	Local maintenance
EV driver	• Authenticate for charging • *Optional:* Pay for charging	Authentication terminal
Electric vehicle	• Control the charging • *Optional:* authenticate for charging	Electric vehicle
Other charging station	• Load balancing within a charging plaza	LAN
Local EMS	• Energy management within the local context (e.g., building)	LAN

2.1 User access management [A.9.2]

The charging station manages access rights for the user groups to allow the CPO to implement the principle of least privileges.

Requirement numbering

Requirements are numbered according to the measures in the security architecture [1] with “-CS” appended for charging station. For instance, requirement AC7-CS implement architecture measure AC7 on the charging station. Because not all

architecture measures concern the charging station, there may be gaps in the numbering.

AC7-CS: Least privileges for the CSMS, EV drivers, electric vehicles, other charging stations, and the local EMS

The charging station shall restrict the privileges of the CSMS, EV drivers and electric vehicles, so that they can access only the functions and data they need.

Remark: There are no requirements on how the privileges are managed. They may be static and only be changeable through software updates. Often the privileges are already restricted by the protocol that is used.

AC8-CS: Local accounts for engineers

If the charging station supports local maintenance, it shall support access control for engineers with local accounts and enforce the corresponding access privileges.

Remark: For charging stations that can maintain a reliable connection with the central systems, it is recommended to use centrally managed, role-based access control. User accounts and roles can then be managed by administrators through the CPO central system.

Different methods can be used for centralized access control, for instance using RADIUS, LDAP, or Active Directory. Charge point operators should choose a method that works with their existing systems.

2.2 System and application access control [A.9.3]

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

AC9-CS: Machine-to-machine authentication for the CSMS, other charging stations and the local EMS

The charging station shall support mutual authentication with passwords or keys for the CSMS, other charging stations, and the local EMS.

AC10-CS: Authentication using passwords for engineers

The charging station shall require engineers to log in with a password. The charging station shall support passwords that are strong enough to resist brute-force attacks.

Remarks: To limit the impact of passwords leaking, it is recommended to use either a unique password for each charging station or centrally managed access control with individual passwords for all engineers.

It is recommended to use a password hashing function, such as Argon2 or PBKDF2, that is resistant against GPU cracking attacks.

AC11-CS: Authentication for EV drivers

The charging station shall require EV drivers to authenticate on the authentication terminal interface using the mechanism chosen by the mobility service provider.

Remark: Different mobility service providers use different mechanisms, such as tokens, RFID cards or mobile apps. It is strongly recommended to choose an authentication mechanism that is resistant to known attacks. Some current mechanisms are vulnerable to attacks such as cloning. To allow these to be changed in the future, the charging stations should support replacing the authentication terminal (see measure OP1 in Section 5.1).

AC12-CS: Machine-to-machine authentication for electric vehicles

If the electric vehicle interface allows functions more advanced than controlling the charging, the charging station shall use mutual authentication with passwords or keys for the electric vehicles. It protects against compromises of the keys and passwords as described in AC5.

Remarks: Passwords and keys are updated according to measure CR2. More advanced functions are usually accessed through the IEC 15118 protocol [6]. This protocol defines a certificated-based authentication mechanism.

3 Cryptography

The charging station uses cryptography for several functions:

- Machine-to-machine authentication for various users (Section 2);
- Hashing passwords used by human users (Section 2);
- Verifying the digital signatures of firmware (Section 4);
- Protecting the confidentiality and integrity of communication (Section 6).

Measures need to be taken to make these cryptographic techniques work well.

3.1 Cryptographic controls [A.10.1]

The charging station uses strong cryptographic keys and algorithms to protect against attacks on the cryptography itself. The charging station supports remote key updates from the central systems allowing keys to be updated on thousands of charging stations.

CR1-CS: Strong cryptographic keys and algorithms

For security functions, the charging station shall use cryptography according to regulations and modern guidelines:

- It only uses the cryptographic algorithms that the ECRYPT – Algorithms, Key Size, and Protocols Report [7] recommends as suitable for new or future systems;
- It uses keys as least as long as the ECRYPT report recommends for near term use (section 4.6 in [7]);
- It only uses a dedicated cryptographic pseudo-random number generator meeting the requirements in the ECRYPT report [7] Section 3.2.3 to generate random numbers for security functions;
- If it uses certificates for authentication, it validates them by checking the signature, the certificate-chain, the revocation status, and the identity of the user or role through the subject name, common name or distinguished name.

CR2-CS: Remote password and key updates

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

Where the charging station uses certificates for authentication or communication security, it shall be able to use certificates issued by the public key infrastructure (PKI) of the CPO.

Remarks: It is allowed that some keys or credentials used for internal purposes cannot be updated remotely. But, as soon as they are used to implement any of the requirements in this document, they must also comply with this requirement.

The certificate used to verify firmware updates (OP9-CS) is issued by the vendor. So, for this certificate the charging station does not need to be able to use certificates from the CPO.

4 Physical and environmental security

4.1 Equipment [A.11.2]

The charging station is protected against tampering by its cover.

PH3-CS: Tamper detection

The charging station shall detect physical tampering by:

- having a cover protecting against physical manipulation, so that attackers without specialized tools cannot reach its internal components without leaving visible traces;
- creating a log event whenever any part of the cover is opened.

Remarks: The log event is part of the OCPP 2.0 specification, as a “Tamper Detection Activated” security event.

Additional measures can be taken in the hardware, firmware and software to strengthen the protection, such as using a trusted platform module (TPM), secure boot and read-only memory.

PH4-CS: Physical access to local maintenance interface only from casing

The charging station shall only allow physical access to the local maintenance interface after its casing has been opened.

Remark: Because of measure PH2, a log event will be created whenever an engineer opens the casing to access the local maintenance interface.

Engineers may access the charging stations through local area network (LAN) in a charging plaza or through a wireless network to avoid the need to open their casing. Wireless access should only be enabled during. If the equipment has wireless capabilities, then those can be enabled and used. Otherwise, a wireless access point can be used.

5 Operations security

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

5.1 Operational procedures and responsibilities [A.12.1]

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

OP1-CS: Future-proof design

The charging station shall have enough memory (RAM and flash) as well as computation power to allow for security updates needed during its lifetime to be installed, under the following assumptions:

- Cryptographic measures are updated following the standards in CR1-CS, in particular the RTU support the key sizes recommended for long term use in Section 4.6 of the ECRYPT report [7];
- Roles and security event types will grow incrementally by up to 50%.

The authentication terminal of the charging station shall be easily and fully replaceable in case stronger authentication is needed for EV drivers.

Remarks: Compliance to the requirement can be shown through performance tests. Tests with current firmware under operational workloads should show that there are enough reserves to extend security functions. Tests with algorithms recommended for long term use in [7] should show that the charging station can run them without affecting operations. It is acceptable if the charging station can only support the long term key sizes for elliptic curve based algorithms, not for RSA-based algorithms.

5.2 Backup [A.12.3]

To support recovery processes, it needs to be possible to reset charging stations to factory defaults. No support for backups is required, as the charging stations do not store important information locally.

OP3-CS: Reset to factory defaults for charging stations

The charging station shall provide a secure method to reset them to factory default settings, including the security settings, in case of problems.

5.3 Logging and monitoring [A.12.4]

To support detection and response to security incidents, the charging station needs to log relevant security events and allow them to be gathered for analysis. Because the security logs are vital for security, they also need to be protected themselves.

OP4-CS: Security events

The charging station shall be able to log security events for the following in a local log:

1. Firmware updates
2. Failed authentication attempts
3. Changes to the system time
4. Booting the device
5. Changes to the security log
6. Changes to security parameters
7. Memory exhaustion
8. Attempts to physically tamper with the device
9. Invalid firmware signatures
10. Invalid certificates
11. Invalid settings for cryptographic protocols such as TLS

The log entries for security events shall include a timestamp, an event description and the user, role or process causing the event.

OP5-CS: Collecting security events

The charging station shall allow to read out the security logs using normal maintenance tools.

The charging station shall be able to send all security logs to the central system. The events shall allow parsing (i.e., easy interpretation) by the central server, avoiding the need to develop a dedicated parser.

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

OP6-CS: Protecting security logs

The charging station shall protect security logs by:

- restricting access by only allowing authorized users to access them;
- having enough storage capacity to store the security logs;
- implementing a rolling security log, in which the entries with the oldest timestamp are discarded first if log storage is full.

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

The charging station should have at least enough storage capacity to store security events for one week if communications with the central system are interrupted, assuming normal operating conditions.

5.4 Control of operational software [A.12.5]

The charging stations support secure software installation procedures by allowing remote updates that are digitally signed.

OP8-CS: Remote firmware updates

The charging station shall allow remote updates from the CPO central system for all security functions, for which updates are expected to be needed. Remote updates allow to:

- Update all cryptographic algorithms and protocols (see CR1-SM);
- Update the cryptographic random number generator (see CR1-SM);
- Add more roles (AC13-SM);
- Change the authorization of roles (see AC13-SM).

OP9-CS: Verification of firmware signatures before installation

The charging station shall be able to verify the integrity and source of firmware updates before installing the firmware by using digital signatures. The vendor digitally signs each firmware release using his private key in a secure environment at their premises.

5.5 Technical vulnerability management [A.12.6]

To support effective vulnerability management, the charging station is hardened, avoids known vulnerabilities and applies input validation.

OP10-CS: Hardening

The charging station shall support hardening by disabling unneeded functions. The charging station shall allow:

- unused user accounts to be removed;
- unused network services to be disabled;
- unused, externally accessible hardware ports to be disabled.

Remark: Internal hardware ports on the charging station do not need to be disabled, although this can help hardening the system even further.

OP11-CS: Known vulnerabilities

The charging station shall only use applications, libraries and communication protocols without known security vulnerabilities.

OP12-CS: Input validation

The charging station shall apply input validation to all data it receives.

Remarks: The charging station developer should make sure their code checks the validity of all received data, including validating if the input values are within the permitted value range. They should regularly check that there are no input validation vulnerabilities in third-party libraries and applications. They should use code reviews and robustness tests for code they develop in-house, such as web interfaces or the implementation of domain-specific protocols such as OCPP [10].

OP13-CS: Hardware assisted measures against exploits

The charging station shall implement the following hardware features if they are available:

- *No-Execute (NX) / Write-xor-execute (W^R):* If the charging station has a Memory Protection Unit (MPU) or Memory Management Unit (MMU), it shall be used to mark code regions as read-only and data sections as non-executable.
- *Address Space Layout Randomization (ASLR):* If the charging station has a Memory Management Unit (MMU), it shall be used to load data and code at different memory addresses every time an application is run.

The software running on the charging station shall be compiled to use the hardware features.

Remark: The Position Independent Code (PIC) or Position Independent Executable (PIE) compiler options should be enabled to be able to use ASLR.

6 Communication security

6.1 Network security management [A.13.1]

The charging station cryptographically protects communication confidentiality on untrusted networks. It restricts access to wireless networks used for local maintenance. It is also resilient against denial-of-service (DoS) attacks, as the charging station can be reached directly from untrusted networks.

CM1-CS: Confidentiality and integrity of network communication

The charging station shall be able to use cryptographic measures to protect the integrity and confidentiality of communication on the WAN interface. The measures allow to verify the source of messages and protect against replay attacks.

CM4-CS: Restriction on wireless communications for local maintenance

If engineers use wireless communication to maintain charging stations, the charging stations shall be able to restrict access to the wireless network using strong passwords.

Remark: Wireless communication may be used for standalone charging stations or in a charging plaza. It is recommended to only turn on the wireless access during the maintenance work.

CM5-CS: Resilience against denial-of-service attacks

The charging station shall be resilient against DoS attacks: it does not become unavailable for long periods of time when network interfaces are flooded with data or when malformed messages are received.

Remark: The charging station may become slower when flooded or when dealing with malformed packets, but it should not crash or reboot.

7 System acquisition, development and maintenance

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

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

SD1-CS: Secure programming practices

The developer shall set up programming practices to ensure the consistent delivery of secure charging stations. The vendor shall:

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

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

Compiler options that should be enabled include:

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

SD2-CS: Security testing during development

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

- Functional testing for all functional requirements;

- Robustness testing of custom protocol implementations;
- Automated web application testing on any web interfaces;
- Automated vulnerability scanning.

Remark: The test plan for charging stations [5] includes a list of test cases that vendors can use to check the implementation of the requirements.

SD3-CS: Support for independent testing

The developer shall support acceptance testing by the CPO or an independent party by:

- allowing the CPO or a third party to audit the development process;
- providing documentation on how the requirements have been implemented;
- making charging stations available for testing;
- providing all keys and credentials needed for testing;
- providing access to source code for code reviews.

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

SD4-CS: Secure configuration guidelines

The developer shall provide guidelines on how to securely configure and operate the charging station, covering at least:

- expected security measures in the operating environment;
- hardening;
- account management;
- setting up security logging.

SD5-CS: Vulnerability handling

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

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

The developer shall inform the CPO about all vulnerabilities found as soon as possible.

Remark: To determine which vulnerabilities are severe, the Common Vulnerability Scoring System (CVSS) can be used. Vulnerabilities with a score of 7.0 or higher would be considered severe and in need of fixing.

The developer may agree with the CPO to use another method to determine the severity of the vulnerabilities, if it can be objectively applied and gives a good indication of the risk.

8 Supplier relationships

8.1 Information security in supplier relationships [A.15.2]

To ensure that the charging station developer protects information that is important for the CPO, it needs to implement an information security management system.

SR1-CS: Protection of customer assets

The developer shall have an information security management system (ISMS) to protect any information that could compromise the security of the CPO, including:

- detailed security designs;
- source code;
- customer-specific keys and credentials.

The ISMS shall be ISO 27001 certified and the certification scope shall cover the development and manufacturing of the charging station as well as any related tools.

9 Information security aspects of business continuity management

9.1 Information security continuity [A.17.1]

To ensure that the security of the EV infrastructure is not compromised during disruptions, the charging station must be designed to fail securely.

BC1-CS: Fail-secure design

The charging station shall be designed to minimize the impact of a failure on security. During a failure the charging station shall:

- not leak confidential information, such as keys or credentials;
- protect the integrity of critical data;
- not allow access controls to be bypassed;
- restore availability as soon as possible.

Remark: Examples of failure are hardware malfunctions, corruption of stored or received data and software crashes. A watchdog can be used to monitor the infrastructure components and to automatically initiate steps to restore availability.

Appendix A: Implementing the requirements in OCPP 2.0

This appendix explains how many of the requirements can be met by implementing the OCPP 2.0 standard [13] used by many charging stations.

Requirements fully covered by OCPP 2.0

The requirements in Table 2 can be fully implemented by following the OCPP 2.0 standard. If the charging station is compliant with OCPP 2.0, it automatically meets these security requirements.

Table 2: Requirements fully covered by OCPP 2.0.

Requirement	Section in [13]	OCPP Implementation
OP4-CS: Security events	Enumeration 2.73	The events in enumeration 2.73 are logged.
OP8-CS: Remote firmware updates	L. Firmware management	OCPP 2.0 defines use cases for remotely updating the firmware.
OP9-CS: Verification of firmware signatures before installation	L.2.L02	The secure firmware update process defined in OCPP 2.0 use case L02 uses digital signatures. Note that to meet the requirement, non-secure firmware updates (use case L03) should be disabled.

Requirements partially covered by OCPP 2.0

The requirements in Table 3 are covered by the OCPP 2.0 as far as they concern the security functions of the OCPP protocol. For security functions not part of the OCPP standard, these requirements need to be implemented independently from the OCPP 2.0 standard.

Table 3: Requirements partially covered by OCPP 2.0.

Requirement	Section in [13]	OCPP Implementation

AC7-CS: Least privileges for the CSMS, EV drivers, electric vehicles, other charging stations, and the local EMS	-	The OCPP protocol implicitly defines the access rights of the CSMC by describing which functions are exposed over OCPP.
AC9-CS: Machine-to-machine authentication for the CSMS	A.1.3.4 – A.1.3.7	OCPP 2.0 offers two profiles. In both profiles the CSMS authenticates using a TLS and a certificate. With the TLS with Basic Authentication profile, the charging station authenticates using HTTP basic authentication and a password. With the TLS with Client Side Certificates profile, the charging station authenticates using TLS and a client-side certificate.
CR1-CS: Strong cryptographic keys and algorithms	A.1.3.5, A.1.3.7 A.1.4.1 L.2.L01	OCPP 2.0 defines algorithms and keys lengths for all cryptographic mechanisms it uses.
CR2-CS: Remote password and key updates	A.2.A01, A.2.A02, A.2.A03, M.2.M05, M2.M06	The passwords and keys that the charging station uses to authenticate to the CMSM can be updated through use cases A01 - A03. All CA certificates can be updated through use cases M05 and M06.
OP5-CS: Collecting security events	Appendix 1, A.2.A04, N.2.N01	For events that are defined as critical in Appendix 1, a notification is sent to the CSMS through use case A04. Logs for other events can be retrieved through the normal logging mechanism (use case N01). Retrieving logs locally is out of scope for OCPP.
CM1-CS: Confidentiality and integrity of network communication	A.1.3.4 – A.1.3.7	In both the TLS with Basic Authentication and TLS with Client Side authentication, the confidentiality

	and integrity of the communication is protected through TLS.

Requirements not covered by OCPP 2.0

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

- AC8-CS: Local accounts for engineers
- AC10-CS: Authentication using individual passwords for engineers
- AC11-CS: Authentication for EV drivers
- AC12-CS: Machine-to-machine authentication for electric vehicles
- PH3-CS: Tamper detection
- PH4-CS: Physical access to local maintenance interface only from casing
- OP1-CS: Future-proof design
- OP3-CS: Reset to factory defaults for charging stations
- OP6-CS: Protecting security logs
- OP10-CS: Hardening
- OP11-CS: Known vulnerabilities
- OP12-CS: Input validation testing
- OP13-CS: Hardware assisted measures against exploits
- CM4-CS: Resilience against denial-of-service attacks
- CM5-CS: Resilience against denial-of-service attacks
- SD1-CS: Secure development process
- SD2-CS: Security testing during development
- SD3-CS: Support for acceptance testing
- SD4-CS: Secure configuration guidelines
- SD5-CS: Vulnerability handling
- BC1-CS: Fail-secure design

Glossary

AD	Active Directory
CPO	Charge Point Operator
CSMS	Charging Station Management System
DoS	Denial-of-Service
EV	Electric Vehicle
LAN	Local Area Network
PKI	Public Key Infrastructure
RADIUS	Remote Access Dial-In User Service
RAM	Random Access Memory
RFID	Radio Frequency Identification
TLS	Transport Layer Security
WAN	Wide Area Network

References

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

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

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

[4] ENCS, "Security risk assessment for EV charging infrastrucure," 2019.

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

[6] ISO, "ISO 15118-1:2019: Road vehicles - Vehicle to grid communication interface - Part 1: General information and use-case definition," 2019.

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

[8] National Institute for Sandards and Technology (NIST), "Special Publication 800-57 Part 1 Rev. 3: Recommendation for Key Management," 2012.

[9] ISO/IEC, "ISO/IEC 19790:2012: Information technology -- Security techniques -- Security requirements for cryptographic modules," 2012.

[10] O. C. Alliance, "Open Charge Point Protocol 2.0," [Online]. Available: https://www.openchargealliance.org/protocols/ocpp-20/. [Accessed 2019].

[11] SEI CERT, "SEI-CERT Coding Standards," [Online]. Available: https://www.securecoding.cert.org/confluence/display/seccode/SEI+CERT+Coding+Standard.

[12] MISRA, "MISRA C software development guidelines for embedded systems," [Online]. Available: http://www.misra.org.uk/.

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