EV-401-2019

Security test plan for EV charging stations

Version 1.0

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
25 October 2019	0.1	Initial draft
6 December 2019	0.2	Update after workshop on testing on 25 November
24 December 2019	1.0	Final version in member project on procuring secure equpiment

ENCS

Table of Contents

1 Introduction

This document provides a plan to test distribution automation (DA) remote terminal units (RTUs) against the security requirements that ElaadNL and ENCS have developed [1].

When the requirements are used, the need arises to evaluate the charging station against the requirements. Most procurement processes include acceptance testing to make sure that the selected charging station does indeed meet all requirements. This document provides a standardized test plan to evaluate the charging stations against the security requirements in [1].

By standardizing the test plan, the test results can be shared between charge point operators. The vendor of the charging station can order a security test according to the test plan. If the charging station passes the tests, the vendor can use the test report to show compliance in all tenders that use the security requirements. This is expected to reduce the cost of testing and can give charge point operators assurance in advance that there are charging stations meeting the requirements.

If the vendor's equipment provides additional security features, then this plan can be extended to include specific testing steps for the corresponding requirements.

The test plan consists of three phases:

1. Functional tests and a vulnerability assessment by the vendor, usually performed during development;
2. A review of development processes and security design and OCPP security conformance testing by an external lab;
3. A penetration test by an external lab.

The term 'test' is used broadly to cover any evaluation activities, including interviews and reviews.

1.1 Scope

The test plan covers the security requirements in [1]. The test plan applies to charging stations that use the OCPP 2.0 protocol and implement the security measures in those standards. Using the test plan for other charging stations requires changes.

Using the test

The test plan is 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 [2].
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 [3].
3. Derive **requirements for components** from the security architecture that can be used to develop or procure the components. Requirements for procuring EV charging stations are available in [1].
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. This document gives a test plans for EV charging stations.
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 [4]. To support this, the architecture is organized by the security objectives in ISO 27001 [4] Annex A.

2 Tests by the vendor

The test plan requires the vendor to perform all routine tests: the functional security tests and an automated vulnerability assessment. This approach is the most cost-effective way to perform these tests. It ensures they can be run on each firmware release.

The full test reports should be made available to an external test lab for review (see Section 3.2.2). The test lab can request further evidence from a test case, such as logs and traffic captures, that show that the test case was passed.

2.1 Functional security tests

The vendor checks requirements not implemented through the OCPP 2.0 standard. The implementation of these requirements is often done in a way that is specific to the vendor. Testing it in an external lab would require extensive setup work and would not be cost-effective.

The vendor is required to check the implementation of the requirements in the Table 1 below against the security design. They should at least run the test cases listed.

Table 1: Functional test cases that the vendor should perform.

Requirement	Required test cases
AC8-CS: Local accounts for engineers	• Check that access privileges are enforced
AC9-CS: Machine-to-machine authentication for the CSMS, other charging stations and the local EMS	• Check that other charging stations can log in with valid credentials • Check that authentication attempts for other charging stations with invalid credentials are rejected • Check that the local EMS can log in with valid credentials • Check that authentication attempts for the EMS with invalid credentials are rejected
AC10-CS: Authentication using passwords for engineers	• Check that engineers can log in with a valid password • Check that authentication attempts with invalid passwords are rejected

AC11-CS: Authentication for EV drivers	• Check that EV drivers can authenticate with the authentication mechanism chosen by the mobility service provider • Check that authentication attempts with invalid credentials are rejected
AC12-CS: Machine-to-machine authentication for electric vehicles *(if applicable)*	• Check that electric vehicles can authenticate with the authentication mechanism specified • Check that authentication attempts with invalid credentials are rejected
PH3-CS: Tamper detection	• Check that a security log event is created when any part of the cover is opened
OP1-CS: Future-proof design	• Check how much memory and computing power the charging station is using under normal operations • Check that the charging station can support TLS connections using AES 256 for communication with the CSMS • Check that the charging station can use elliptic curve cryptography with keys of length at least 512 bits for setting up TLS connections to the CSMS
OP3-CS: Reset to factory defaults for charging stations	• Check that the charging station can be reset to factory defaults with the specified process
OP5-CS: Collecting security logs	• Check that the security logs can be read out from the local maintenance interface
OP6-CS: Protecting security events	• Check that user access to the security logs is restricted (if applicable) • Check that the charging station security log is rolling

2.2 Automated vulnerability assessment

In the automated vulnerability assessment, the vendor checks if the charging station has any known vulnerabilities through vulnerability scanning or suffers from input validation or resilience issues through robustness testing.

2.2.1 Vulnerability scanning

During vulnerability scanning, the vendor runs an automated scanner on the charging station, both on the WAN interface and on any local IP-based interfaces. The scanner report is then checked according to the test cases in the following table.

Table 2: Test cases for vulnerability scanning.

Requirement	Test cases
CR1-CS: Strong cryptographic keys and algorithms	• Check that all cryptographic algorithms, used in e.g. SSH or TLS, are according to the requirement
OP10-CS: Hardening	• Check that only the documented network services are open • Check that only the required user accounts are active
OP11-CS: Known vulnerabilities	• Check that the charging station does not have any outdated software installed for which there are known vulnerabilities
CM1-CS: Confidentiality and integrity of network communication	• Check that all network services discovered are protected using the network security measures defined in the security design

2.2.2 Robustness testing

The vendor uses robustness testing to check for input validation issues through fuzzing and resilience errors through flooding. It is recommended to also fuzz the OCPP implementation, but this is not required.

Table 3: Test cases for robustness testing.

Requirement	Test cases
OP12-CS: Input validation	• Fuzzing of the TCP/IP stack • Fuzzing of the TLS implementation

	• If the charging station has a web interface: scanning for known web vulnerabilities using a web vulnerability scanner
CM4-CS: Resilience against denial-of-service attacks	• Flooding the TCP/IP stack with large amounts of data

3 Conformance tests by an external lab

An external test lab tests conformance to the requirements through three activities:

- A review of security of the vendor development processes;
- A technical review of the security design and implementation;
- Functional tests of the security requirements implemented through OCPP.

The tests are based on information provided by the vendor and independent testing. The result of the requirements-based test is a simple pass or fail per requirement. A pass is given if the tests clearly show the measures required are implemented. A fail is given if the tests show that the measures have not been implemented or if there was not enough information to determine if the measures were implemented.

A charging station is only considered to conform to the procurement requirements in [1] if it gets a pass for all requirements.

3.1 Development process review

The assessment of development processes checks that the vendor has implemented all required measures for secure development. Vendors are required to deliver documentation on their processes and the test lab reviews it. Then the test lab asks follow-up questions in a vendor interview.

3.1.1 Review of development process documentation

For the vendor documentation review, vendors are required to deliver the documentation in Table 4. The test lab then checks that the documented processes include the required security measures.

Table 4: Documentation the vendor must provide for the assessment of development processes.

Requirement	Documentation to be provided
SD1-CS: Secure programming practices	• Secure coding guidelines • Training program for developers • Description of process for code reviews • Description of issue tracking method and tools • Description of version control method and tools

	• Description of compiler security settings for the RTU firmware
SD2-CS: Security testing during development	• Security test plan for the charging station • Test reports for firmware version evaluated
SD3-CS: Support for acceptance testing	*No documentation required*
SD4-CS: Secure configuration guidelines	• Secure configuration guidelines
SD5-CS: Vulnerability handling	• Description of process for vulnerability handling • Examples of vulnerability notifications
SR1-CS: Protection of customer assets	• ISO 27001 certificate • Statement of applicability for certification • Summary of the risk assessment

3.1.2 Development processes interview

After reviewing the documentation, the vendor has provided, the test lab asks follow-up questions on the development processes in an interview. The interview takes at least two hours. The vendor is responsible for ensuring the right staff is available to answer questions. It is recommended they include at least:

- someone responsible for secure development processes;
- developers working on the charging station;
- a security officer responsible for the ISMS.

3.2 Technical security review

The test lab reviews the technical security design following the same approach as for the development processes. First documentation the vendor delivers documentation and the test lab reviews it. Then the test lab asks additional questions in an interview.

3.2.1 Review of technical design

For the design review, vendors are required to deliver the documentation listed in Table 5. Evaluators check that according to the documentation provided, the security design meets the requirements.

Table 5: Documentation the vendor must provide for the review of technical documentation.

Requirement	Documentation to be provided
AC7-CS: Least privileges for the CSMS, EV drivers, electric vehicles, other charging stations, and the local EMS	• List of users and their access rights
AC8-CS: Local accounts for engineers	• Description of access control method • List of default users with their privileges
AC9-CS: Machine-to-machine authentication for the CSMS, other charging stations and the local EMS	• Description of authentication method for other charging stations and the local EMS (if applicable)
AC11-CS: Authentication for EV drivers	• Description of authentication method for EV drivers
AC12-CS: Machine-to-machine authentication for electric vehicles	• Description of authentication method for electric vehicles

CR1-CS: Strong cryptographic keys and algorithms	• Cryptographic algorithms and key lengths used, including those for:
	  ○ Password hashing (AC10-CS)
	  ○ Verifying firmware signatures (OP9-CS)
	  ○ Communication security (CM1-CS)
	• Random number generator used, including method for seeding it

CR2-CS: Remote key updates	• Description of remote password and key update process for passwords and keys not covered by the OCPP standard
PH3-CS: Tamper detection	• Drawings of tamper detection sensors

PH4-CS: Physical access to the local maintenance interface only from casing	• Drawing showing physical security of the charging station

OP1-CS: Future-proof design	• Hardware specification including
	  ○ Processor
	  ○ RAM memory
	  ○ Persistent memory (e.g. flash)

OP3-CS: Reset to factory defaults for charging stations	• Description of process to reset the charging station to factory defaults
OP6-CS: Protecting security events	• Description of measures taken to protect the security logs
OP10-CS: Hardening	• List of user accounts with their use • List of network services with their use • List of hardware interfaces with their use
OP11-CS: Known vulnerabilities	• List of third-party libraries and applications used with their versions
OP13-CS: Hardware assisted measures against exploits	• Description of hardware security features on the charging station processor used • Description of the compiler security setting for charging station firmware
CM1-CS: Confidentiality and integrity of network communication	• Description of encryption and authentication measures for protocols on WAN other than OCPP
CM4-CS: Restriction on wireless communications for local maintenance	• Description of measures to restrict access to wireless networks (if applicable)
BC1-CS: Fail-secure design	• Description of watchdog implementation

3.2.2 Review of technical implementation

For the technical implementation review, vendors are required to deliver the reports of the tests in Section 2. The grid operator checks that according to the test reports, the security measures are implemented as designed.

3.2.3 Technical interview

Like for the development processes, the test lab follows up the documentation review with an interview. The interview takes at least two hours. The vendor is responsible for ensuring the right staff is available to answer questions. It is recommended they include at least:

- the product owner responsible for the security roadmap;
- the architect responsible for the security design;
- developers responsible for implementing security features;
- testers that performed the security tests in Section 2.

3.3 OCPP 2.0 security conformance tests

The external test lab independently checks conformance to the security requirements in OCPP 2.0. The charging station is tested against a reference implementation of a CSMS. The vendor must support integrating the charging station into this CSMS, for instance by configuring the communication and loading the correct root certificates.

The OCPP 2.0 compliance testing for security covers the requirements and test cases in the table below. These can be executed as part of broader OCPP 2.0 compliance test covering also non-security requirements.

Table 6: Test cases for OCPP 2.0 security conformance testing.

Requirement	Required test cases
AC9-CS: Machine-to-machine authentication for the CSMS, other charging stations and the local EMS	• Check that the central system can authenticate to the charging station with a valid certificate • Check that the central system cannot authenticate to the charging station if its certificate is expired • Check that the central cannot authenticate to the charging station if there is no valid chain to a CSO root certificate on the charging station • Check that the central system cannot authenticate to the charging station if the subject name does not contain the IP address or URL of the central system

	• Check that the central system properly authenticates to the central system given the security profile used • Check that the charging station refuses to connect to an CSMS that does not use TLS
CR1-CS: Strong cryptographic keys and algorithms	• Check that the charging station uses only the allowed algorithms for TLS
CR2-CS: Remote key updates	• Check that the central system can update the charging station password or key according to use case A01 or A02 in [5] • Check that the central system can update its own certificate when it will expire according to use case A03 in [5] • Check that the central system can update the root certificate according to use case M05 in [5]
OP4-CS: Security events	• Check that the charging station logs all the security events listed in Section 2.73 in [5]
OP5-CS: Collecting security events	• Check that the charging station notifies the central system of critical security events according to use case A04 in [5] • Check that it is possible to read out the security event log according to use case N01 in [5]
OP8-CS: Remote firmware update	• Check that the charging station firmware can be updated according to use case L01 in [5]
OP9-CS: Verification of firmware signatures before installation	• Check that the charging station aborts the firmware update when it receives an invalid firmware signing certificate when following use case L01 in [5] • Check that the charging station rejects a firmware update with an invalid signature when following use case L01 in [5] • Check that the firmware cannot be updated through the non-secure firmware update use case L02 in [5]

CM1-CS: Confidentiality and integrity of network communication	• Check that the charging station supports secure communication through the TLS with basic authentication or TLS with client-side authentication profiles as define in [5] Section 1.3

4 Penetration tests by an external lab

After the conformance tests have checked that all security functions are implemented, the penetration tests check that attackers cannot bypass them.

The tests are time boxed. Testers are given a fix number of days to find vulnerabilities. They choose how to spend those days based on a risk assessment. While the requirements-based testing has a broad scope to cover all requirements, the penetration tests go in-depth on the functions where tester expect the highest risks. Testers used the information from the vendor and conformance tests to assess these risks.

4.1 Code review on WAN interface

The main penetration test activity is to do a code review to find input validation vulnerabilities on the WAN interface. The WAN interface is singled out, because attacks on this interface have the highest impact. They can affect large number of charging stations.

The tester is given the charging station source code and asked to search for vulnerabilities on the WAN interface that can be exploited without credentials. The tester should investigate how data is passed from the modem to the library that implements TLS. Input validation errors in this process could be exploited without credentials. The TLS library itself is out of scope if a mature and tested library is used.

The reason for this approach is that to exploit a charging station on the WAN interface, attackers must find vulnerabilities in the authentication procedure. The attack service on the WAN interface limited. If well-hardened, only OCPP is used on it. The OCPP application layer can only be reached after authenticating with a password or client-side certificate (after which a user has full access to the charging station). So, an attacker must find a vulnerability to bypass this authentication.

The time available for the code review is three days.

4.2 Physical penetration test

The physical penetration test checks that the tamper detection measures on the charging station cannot be bypassed by attackers with moderate resources. The main goal of the test is to ensure there are no easy possibilities for fraud or for reaching internals of the charging station.

The time available for the penetration test is two days. Only tools that can be bought with moderate means are used.

Appendix A: Tracking of requirements

The table below shows which requirements are checked by which test activities. The penetration test is not included, as it is not aimed at specific requirements.

	Functional security tests	Automated vulnerability assessment	Development process review	Technical security review	ÒCPP 2.0 Security conformance test
AC7-CS: Least privileges for the CSMS, EV drivers, electric vehicles, other charging stations, and the local EMS				X	
AC8-CS: Centrally managed, role-based access control for engineers	X			X	
AC9-CS: Machine-to-machine authentication for the CSMS, other charging stations and the local EMS				X	X
AC10-CS: Authentication using passwords for engineers	X			X	
AC11-CS: Authentication for EV drivers	X			X	
AC12-CS: Machine-to-machine authentication for electric vehicles	X			X	
CR1-CS: Strong cryptographic keys and algorithms		X		X	X

	Functional security tests	Automated vulnerability assessment	Development process review	Technical security review	ÒCPP 2.0 Security conformance test
CR2-CS: Remote key updates				X	X
PH3-CS: Tamper detection				X	
PH4-CS: Physical access to local maintenance interface only from casing				X	
OP1-CS: Future-proof design	X			X	
OP3-CS: Reset to factory defaults for charging stations	X			X	
OP4-CS: Security events				X	X
OP5-CS: Collecting security events	X			X	X
OP6-CS: Protecting security logs	X			X	
OP8-CS: Remote firmware updates				X	X
OP9-CS: Verification of firmware signatures before installation				X	X
OP10-CS: Hardening		X		X	
OP11-CS: Known vulnerabilities		X		X	
OP12-CS: Input validation		X		X	

	Functional security tests	Automated vulnerability assessment	Development process review	Technical security review	ÒCPP 2.0 Security conformance test
OP13-CS: Hardware assisted measures against exploits				X	
CM1-CS: Confidentiality and integrity of network communication		X		X	X
CM4-CS: Restriction on wireless communications for local maintenance				X	
CM5-CS: Resilience against denial-of-service attacks		X		X	
SD1-CS: Secure programming practices			X		
SD2-CS: Security testing during development			X		
SD3-CS: Support for acceptance testing			X		
SD4-CS: Secure configuration guidelines			X		
SD5-CS: Vulnerability handling			X		
SR1-CS: Protection of customer assets			X		

	Functional security tests	Automated vulnerability assessment	Development process review	Technical security review	ÒCPP 2.0 Security conformance test
BC1-CS: Fail-secure design				X	

References

[1] ENCS, "EV-301-2019: Security requirements for procuring charing stations," 2019.

[2] ENCS, "EV-101-2019: Security risk assessment for EV charging infrastructure," 2019.

[3] ENCS, "EV-201-2019: Security architecture for EV infrastructure," 2019.

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

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