ElaadNL

Security requirements for Home Energy Management Systems (HEMS)

Version 1.0

20 August 2025

The European Network for Cyber Security (ENCS) is a non-profit member organization that brings together critical infrastructure stake owners and security experts to deploy secure European critical energy grids and infrastructure. Founded in 2012, ENCS has dedicated researchers and test specialists who work with members and partners on applied research, defining technical security requirements, component and end-to-end testing, as well as education & training.

Version History

Date	Version	Description	Authors
25 July 2025	0.1	Internal draft	Amber Cok, Anne Anggraeni, Maarten Hoeve
27 July 2025	0.2	First complete draft shared with ElaadNL	Maarten Hoeve
12 August 2025	0.3	Updated after comments from Ton Smets (ElaadNL)	Maarten Hoeve
18 August 2025	0.4	Updated after comments from Arjan Wargers (ElaadNL)	Anne Anggraeni
20 August 2025	1.0	Complete draft shared with ElaadNL	Anne Anggraeni

ENCS

Table of Contents

1 Introduction

ElaadNL and the Flexiblepower Alliance Network (FAN) are working on a project to develop and test connectors for home energy management systems (HEMS).

HEMS are becoming increasingly popular with consumers to manage high-power devices in their homes, such as charge points, PV inverters, heat pumps, and home batteries. HEMS can also help with the energy transition by providing TSOs and DSOs access to flexibility at consumers. The HEMS can for instance be used to make devices react to dynamic prices or support in congestion management.

But there is a lack of standardization for connecting the HEMS to the devices it manages. Protocols such as Modbus are widely used, but these are not secure.

ElaadNL and the FAN want to support the interoperable and secure development of HEMS by developing and testing open-source software connectors that enable Home Energy Management Systems (HEMS) to communicate with Flexible Energy Intensive Devices (FEIDs) using standardized protocols. FEIDs include charge points, PV inverters, heat pumps, and home batteries.

ElaadNL and the FAN are starting a Request for Proposal (RfP) for 5 such connectors, supporting different communication protocols:

1. S2 / PEBC
2. Matter 1.4
3. EEBus (SHIP / SPINE)
4. Modbus converter
5. OCPP 2.1 proxy

They have asked ENCS to develop cybersecurity requirements that can be given to these developers in the RfP.

1.1 Scope

Security requirements cover connectors to be developed (see Figure 1). The requirements cover authentication and secure communication between the HEMS and the FEIDs but also generating the relevant security log events.

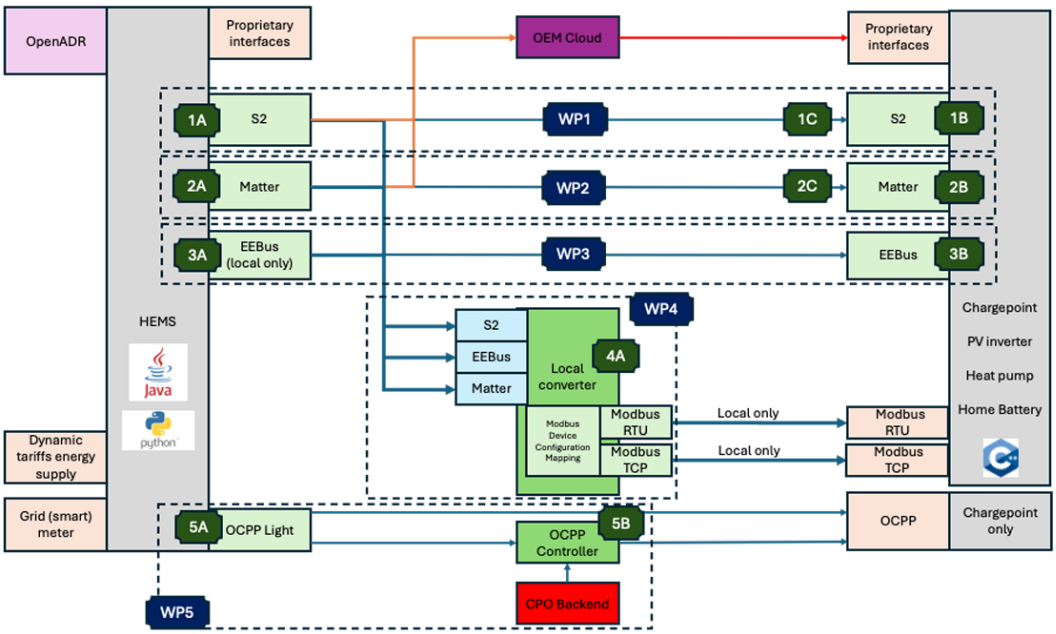

Figure 1: HEMS architecture.

2 Risk assessment

To develop security requirements, a risk assessment was performed on the HEMS by analysing the relevant threat actors, threats, and impact.

2.1 Threat actors

The main threat actors we are concerned with are nations' state actors trying to disrupt the electricity system through load altering attacks. In hybrid warfare scenarios, hostile nation states may be interested in causing power outages. One way in which they can cause outages is by switching a lot of load or generation at consumers to cause imbalances or congestion problems.

Criminal groups are probably less of a threat, but they could still target HEMS and FEIDs for several reasons:

- To collect devices for IoT botnets.
- For ransomware attacks
- For manipulating market prices by switching power use

Note that the HEMS cannot directly be used for fraud, as the billing of the electricity used is through the smart meter.

2.2 Threats

2.2.1 Unauthorized access

Any device on the home network will be able to reach the HEMS and FEIDs. The primary threat is other devices in the home network gaining unauthorized access to the HEMS but especially to the FEIDs.

If an attacker manages to connect to the HEMS pretending to be a FEID, they can send back incorrect information. For instance, they can make it look like the device has reduced power use when it has not.

Conversely, if an attacker manages to connect to the FEIDs, they can directly give a control signal to increase or decrease power use.

2.2.2 Communication threats

If attackers cannot gain direct access to the HEMS or FEIDs, they can try to reach their goal by attacking the communication between them.

Various attacks are possible, such as:

- Eavesdropping on messages
- Manipulating messages
- Spoofing messages
- Replaying messages
- Man-in-the-middle attacks

- Flooding attacks to create a denial-of-service condition
- Denial-of-service attacks through malformed or unusual messages

Attackers will need some control over traffic in the home network to perform these attacks. So, depending on the configuration of the home router, such attacks could be more complex to perform.

But if successful, they can in the worst case give attackers unauthorized access through an indirect router or allow attackers to control power by manipulating control signals. Of slightly less impact would be if a denial-of-service attack would block or delay communication between the HEMS and the FEID.

2.2.3 Attacks on pairing

Another way to gain unauthorized access would be to attack the pairing process between the HEMS and the FEID. Examples of such attacks would be:

- Man-in-the-middle attack during pairing. During the pairing process a hostile device pretends to be the HEMS to the FEIDs, and the FEID to the HEMS, so that it is paired with both and now is in the middle of their connection. A well-known real-world example is a man in the middle attack on Bluetooth Just works, where two legitimate devices pair without user authentication, the attacker can intercept the pairing by creating two separate connections. In Bluetooth, there exist more MitM attacks, also on Bluetooth versions that include pairing mechanisms with secure authentication, such as the KNOB attack[1]. In this attack, the pairing is intercepted and forced to use an encryption key with 1 byte of entropy, which makes it easier for the attacker to brute force the key.
- Tricking the user to reset the pairing. A hostile device disrupts communication between the HEMS and the FEID, and makes the user think that there is a problem with the pairing (e.g. by creating pairing related error messages). The user tries reset the pairing, and then the attacker performs a man-in-the-middle attack.
- Impersonation or spoofing attacks, where the attacker pretends to be the trusted device directly. A real-world example is BLESA[2] in BLE (Bluetooth Low Energy), where the attacker exploits the security in the authentication mechanisms during the reconnection phase of two legitimate devices. The victim device connects to the device of the adversary instead of the legitimate one. Another well-known example is the Evil Twin attack in WiFi, where a device connects to an access point that mimics a known trusted network by using the same SSID.

2.2.4 Privilege escalation

Another indirect threat is that someone uses that HEMS to get access to functions on the FEID that the HEMS does not need. The HEMS normally would only need access to flexibility functions on the FEID for demand response.

[1] https://knobattack.com/

[2] https://www.usenix.org/conference/woot20/presentation/wu

But the device may provide additional functions. Charging stations for instance allow transactions to be performed over OCPP. Inverters allow electrotechnical settings to be configured through their management interfaces, such as how it reacts to changes in the grid frequency. Access on the FEID should normally be restricted so that the HEMS cannot access them.

The threat is that an attacker first compromises the HEMS system and then uses the lack of access control or a vulnerability to gain access to these other functions.

2.3 Impact

As the HEMS is connected to the power grid, a simultaneous attack by malicious actors to multiple vulnerable HEMS poses a large-scale risk to both energy providers and consumers. Based on the RVO report, the following impacts have been identified because of an attack on HEMS.

2.3.1 Loss of power in the power grid

Hackers who gain access to HEMS can remotely manipulate the power output of appliances, which can cause significant changes to the power demand. These changes overload transformers and power lines leading to an unbalanced power grid. As a result, power grid components are damaged, and power supply is lost.

For a limited number of compromised HEMS, this could mean a local power grid failure in which the scale of impact is localized to neighbourhoods and towns. However, large-scale interference with HEMS can significantly change energy consumption, resulting in significant deviations to frequency. The scale of impact can reach the European level if such an attack is conducted on multiple vulnerable HEMS across European countries.

2.3.2 Financial impact on energy companies

Manipulating the power output of appliances connected to the HEMS means causing significant changes to the energy demand and consumption. This will cause deviations to energy predictions by energy companies and lead to inaccuracies in financial decisions on the energy markets.

Hackers can turn on appliances that are not supposed to be on or vice versa, which causes either a spike or drop in energy demand. For energy companies, this would mean unexpected excess or shortage of power purchased. This is a high financial risk as shortage of power would mean unexpected expenses to purchase additional power, while excess of power means these companies have spent more than necessary.

2.3.3 Loss of power for consumers

Unauthorized manipulation of the HEMS not only negatively impacts the power grid and energy companies but also impacts the consumers. Changing HEMS controls causes appliances to not function as intended. Furthermore, this impact may be exacerbated by the failure of the power grid due to manipulation of HEMS controls. On the one hand, a localized attack on individual HEMS can cause consumers to experience disruptions in their day-to-day activities, such as malfunctioning heaters, boilers, and charging points.

On the other hand, power grid failures can cause prolonged loss of power to entire communities.

3 Security requirements

This section defines the security requirements for the connectors. The requirements are based on EN 18031, the harmonized standard for the cybersecurity delegated act of the Radio Equipment Directive. EN 18031 was chosen because any equipment using radio communication already should meet this standard. Additionally, it is expected to be the basis of future standards for the Cyber Resilience Act. The requirements below should cover all requirements in EN 18031 relevant to the connector. See the Annex for more information.

3.1 Functional security requirements

This section describes the functional security requirements for the components. The requirements are formulated in a protocol independent manner. See Section 4 for guidance on how they can be implemented in the protocols considered for the RfP.

3.1.1 Access control

- *[ACM-1 Applicability of access control]* The connector shall apply access control on all functions it exposes.
- *[ACM-2 Appropriateness of access control]* The connector shall ensure that only authorized entities have access to the functions it exposes.

Implementation guidance: Some of the supported protocols are designed to give access to functions that are not needed by the HEMS. For instance, OCPP does not only allow a HEMS to set profiles for smart charging. It also

allows a charging station management system to handle transactions. The HEMS should not be able to access such functions.

The connectors can restrict the access in two ways:

- Only implement the functionality required for the use cases in the RfP. If other functions are supported by the protocol, these are blocked or not implemented in the connector.
- Implement some kind of role separation, so that the other devices can be given a role that only gives access to the functions it needs.

Not all protocols support role separation, as explained in Section 4. In those cases, the first access control method should be used.

3.1.2 Authentication and pairing

- *[AUM-2-A Pairing]* The connector shall implement a mechanism to pair with FEIDs over the selected protocol. The pairing mechanism selected shall be resistant against man-in-the-middle attacks. The pairing shall establish keys or other credentials on the HEMS and FEIDs that can be used for future authentication.

- *[AUM-2-B Authentication after pairing]* After pairing has been completed, the connector will only accept mutually authenticated connections using the keys or credentials established during pairing.
- *[AUM-3 Certificate validation]* If certificates are used for authentication, the connector shall validate all relevant properties of the certificate, such as the signature, the certificate chain, validity period, and the subject alternate name.
- *[AUM-4 Forgetting the pairing]* The connector shall allow the HEMS and FEID to forget the pairing, so that the user can pair the FEID again.

3.1.3 Secure communication channel

- *[SCM-1 Applicability of secure communication mechanisms]* Once a pairing has been established, the connector shall only use secure communication mechanisms.
- *[SCM-2 Appropriate integrity and authenticity protection for secure communication mechanisms]* After pairing, the connector shall protect the integrity and authenticity of application layer data through cryptographic message authentication.
- *[SCM-3 Appropriate confidentiality protection for secure communication mechanisms]* After pairing, the connector shall protect the confidentiality of application layer data through encrypting it.
- *[SCM-4 Appropriate replay protection for secure communication mechanism]* After pairing, the connector shall protect all application layer data against replay attacks.

Implementation guidance: Most protocols will implement these requirements through the use of Transport Layer Security (TLS), as explained in Section 4.

Application layer data would be the data exchanged by the application layer protocol. Lower layer protocols should be protected as much as possible. But often it is not possible to secure all the headers and messages used by such protocols.

3.1.4 Logging

- *[LGM-1 Applicability of logging mechanisms]* The connector shall allow the HEMS and FEIDs to log any activities relevant to privacy assets. The connectors shall also allow to log the following security events:
    - Successful pairings
    - Failed pairing attempts
    - Updates of communication credentials
    - Failed authentication attempts

3.2 Non-functional security requirements

This section gives non-functional security requirements on the use of cryptography, secure development, and testing during development.

3.2.1 Secure software development

- *[GEC-6 Secure development training]* All developers involved in the development of the connectors shall receive appropriate training in secure development. The training shall cover the languages and technologies used for the connector. The supplier shall provide evidence of the trainings. In particular, developers shall be trained to apply proper input validation to all data received by the connector.

3.2.2 Security testing during development

- *[GEC-1-A No known vulnerabilities]* When the connector is delivered, it shall not contain publicly known exploitable vulnerabilities, unless their risk has been mitigated to an acceptable level and ElaadNL and FAN have accepted the mitigation.
- *[GEC-1-B Software composition analysis]* The developer shall run automated Software Composition Analysis (SCA) tools to find publicly known vulnerabilities in the connector's dependencies, such as libraries.
- *[GEC-1-C Resolving vulnerabilities]* ElaadNL and FAN will run the SonarQube advanced security module on the delivered code. The supplier shall resolve any issues found that are classified as medium or higher.
- *[RLM-1 Robustness tests]* The developer shall perform robustness tests, including fuzzing and flooding, on the connector during development.

Implementation guidance: SCA can be done through the SonarQube SCA module or open-source tools, such as OWASP dependency check.

3.2.3 Cryptography

- *[CRY-1 Best practice cryptography]* The connector shall use best practice cryptography for implementing security mechanisms.
- *[CCK-1 Key length]* Keys used by the connector shall support a minimum security strength of 112 bits.

Implementation guidance: Guidance on cryptographic algorithms and key lengths is given in:

- The EUCC scheme Guidelines on cryptography – Agreed Cryptographic Mechanisms [1]
- the ANSSI selection guide for cryptographic algorithms [2] and rules and recommendations on the choice and parameters of cryptographic algorithms [3]
- the BSI technical guideline *Cryptographic Mechanisms: Recommendations and Key Lengths* [4]
- the NIST *Recommendation for key management* [5]

The latest version of these reports should be followed.

Algorithms and key sizes should be used that are recommended for new systems at the time of deployment, and preferably also for the full lifetime of the product.

A dedicated cryptographic (pseudo-)random number generator should be used to generate random numbers for all security functions.

3.2.4 Security documentation

- *[GEC-2/5 Security documentation]* The developer shall provide documentation on how to securely integrate the connector into a HEMS or FEIDs. The documentation shall describe how to use all the required security functions. The documentation shall describe the network services that the connector exposes and the steps that HEMS and FEID developers should take to harden these interfaces.
- *[AUM-5/6 Documentation on initializing passwords]* The documentation shall include guidance on how to initialize passwords and other credentials used by the connector, so that they are initialized to a unique value for each device and are resistant against brute-force attacks.
- *[CCK-2/3 Documentation on initializing keys]* The documentation shall include guidance to initialize cryptographic keys to a unique value for each device using a cryptographic random number generator.

4 Implementation of the requirements

This section describes how the requirements could be implemented in the four protocols considered for the connectors: Matter, EEBus, S2, and OCPP.

Table 1: Implementation of the security requirements in the different protocols. Green means that the feature is fully supported. Yellow means that it can be supported possibly with some workarounds in the connector implementation. Red means not supported.

	Matter	EEBus	S2	OCPP
Access control	Supported through access control lists	Connector should only implement HEMS functions	Connector should only implement HEMS functions	Connector should only implement HEMS functions
Authentication and pairing	Supported through Commissioning	Supported (with some restrictions on verification methods)	Not supported	Pairing not supported. Authentication through TLS
Secure communication	Supported on the application layer	Supported through TLS	Not supported	Supported through TLS
Logging	Logging supported but not all security events logged	Not supported	Not supported	Supported
Cryptography	Supported	Mostly supported but does use legacy SHA-1	Not supported	Supported

4.1 Matter

Matter is a communication standard for HEMS operating over TCP/IP, where WiFi, Ethernet, or Thread networks are supported. For commissioning, Bluetooth Low Energy (BLE) is used. It is built to support bridges that allow non-Matter devices to connect to the home network and enable the use of other protocols.

A Matter **node** is defined as a logical entity with a Node ID and operational credentials that support the Matter protocol stack. A Matter **device** is a piece of equipment and may contain one or more nodes.

During commissioning, a node that performs commissioning is referred to as Commissioner. This can typically be a mobile phone connected to the HEMS network. A Commissionee is the entity that is being commissioned to become a node in the network.

4.1.1 Access control

Matter's device access control system holds the principle of least privilege. Access to a Node's endpoint is denied by default unless access is explicitly granted by assigning the required privileged level (section [6] 6.6).

Each node holds an Access Control List (ACL) containing entries pertaining to the granted privilege level, and a list of Nodes in which the entry applies. An Access Restriction List (ARL) may also be configured. Its entries include an endpoint and list of restricted elements.

The connector can meet the access control requirement in ACM1 by using ACLs that only give the HEMS access to the functions it needs.

4.1.2 Authentication and pairing

In Matter, the pairing is done through a commissioning process, which meets requirement AUM-2-A. Matter devices are authenticated using two certificates (see [7]):

- The **device certificate** provided by the manufacturer before the device is shipped
- The **operational certificate** established during commissioning

The device certificate is used to attest that the device is a valid Matter device. The operational certificate is used to identify the device within a Matter network (called a Fabric). The operational certificate is provided by a Commissioner in the Fabric. In the HEMS architecture, the HEMS would probably act as a Commissioner for the FEIDs. That would mean that the connector on the HEMS side needs to implement a process to securely provide operational certificates to the FEIDs.

During commissioning, a Device Discovery process first establishes a connection between Commissioner and Commissionee, in which the user will be prompted to input the onboarding payload and start a PASE secure commissioning session.

After that, the Commissionee is authenticated through an out-of-and secret that is part of the Onboarding Payload. The onboarding payload of each device contains Vendor and Product ID as unique device identifiers, a passcode required to initiate the PASE process, and a Device Attestation Certificate (DAC) embedded in the device by the manufacturer (see [6]section 5.1). The Onboarding Payload can have different formats (see [7]):

- Human-readable (numeric string)
- Machine-readable (QR code and NFC tag)

Node operational credentials are managed by the Node Operational Credentials Cluster (section 6.4.2), which allows an Administrator to add, update, or remove node credentials.

After the commissioning process, the operational certificate is used for authentication, meeting requirement AUM-2-B.

Matter states Devices and Nodes have a factory reset capability to remove all security, privacy, and key data created during or after commissioning (section 13.4). For example, a NOC is wiped if a Node is factory reset. This functionality meets requirement AUM-4.

4.1.3 Secure communication channel

Matter supports secure communication channels during commissioning and message exchanges on the fabric.

Once a Matter node obtains operational credentials and connects to the operational network (either WiFi or Thread), a secure message communication between nodes is established through certificate-authenticated session establishment (CASE). The NOC is used in CASE to authenticate identities and show proof of possession of private keys.

Matter supports message protection mechanisms such as message security and message privacy. Message security protects data confidentiality and integrity by encrypting the message payload with AES encryption key. Message privacy obfuscates message header fields such as message counter, source ID, and destination ID with privacy keys.

4.1.4 Logging

Secure channel protocols provide support for status reporting (see [6] section 4.11). Several security events that are reported are:

- Indicate successful session establishment
- Errors during session establishment
- Errors after session establishment
- Indicate session termination

The access control cluster generates events for any changes to ACL attribute data performed by an administrator (see [6] section 9.10). Changes include added entries, changed entries, and removed entries.

This partially meets the LGM-1 logging requirements. Security events related to pairing or updates of credentials do not seem to be included.

4.1.5 Cryptography

Matter uses industry standard cryptographic algorithms to protect communication security and integrity (see [7]). The cryptographic suite is listed as follows:

- **Integrity hash**: SHA-256
- **Message security:** AES-CCM 128 bit
- **Message privacy:** AES-CTR
- **Message authentication:** HMAC-SHA-256
- **Digital signatures and key exchanges:** ECC Curve NIST P-256

4.2 EEBus

EEBus is an open-source communication standard facilitating the interoperability between smart home devices and energy management systems. It operates over TCP/IP in the LAN.

The EEBus architecture consists of communication layer and information layer. The standard uses SHIP (Smart Home IP) protocol to transport messages in the communication layer, while SPINE (Smart Premises Interoperable Neutral message Exchange) covers the information layer. A SHIP node refers to a logical device communicating via the SHIP protocol.

4.2.1 Access control

EEBus does not support a role-based access control model. Hence, requirements ACM-2 would have to be met by only implementing the functionality needed by the HEMS in the connector and blocking all other access to the FEID.

4.2.2 Authentication and pairing

EEBus SHIP requires the use of mutual authentication with TLS ([8] section 9). This meets requirement AUM-2-B.

A SHIP node is identified through the Subject Key Identifier (SKI) extension in the certificate, which contains a SHA-1 hash of the public key (see [8] Section 12.2).

EEBus SHIP allows both self-signed certificates and certificates from a PKI (see [8] Section 12.1.1). The idea is that during pairing the user checks the public key in the certificate SKI using one of the following four verification methods in order of ascending user trust level (see [8] Section 12.3):

1. **Auto accept:** during a certain time window, the SHIP node accepts any certificate it receives. Only one certificate is accepted during that time. After that, the window is closed. The window could for instance be triggered by pushing a button on the node.
2. **User verify:** when a SHIP node receives an unknown certificate, it informs the user by showing its SKI on a screen.
3. **Commissioning:** the trusted SKI values are loaded into the SHIP node using a commissioning tool.
4. **User input:** the user enters the trusted SKI values into the SHIP node.

Once a SHIP node has verified a public key, it trusts the certificate. The SHIP node stores the verification method that was used.

The user trust level describes how trustworthy the pairing method is. For HEMS use, we would only recommend using the Commissioning and User input methods. The other methods do not meet requirement AUM-2-A as they would be vulnerable to man-in-the-middle attack. (This policy could be implemented by setting a minimum trust level for power control operations. There is already a minimum trust level of 32 for commissioning over SHIP, see Section 12.3.2.)

Alternatively, a PIN can be used as a second authentication factor (see Sections 12. 5 and 13.4.4.3). The PIN would also allow weaker but more user-friendly authentication methods such as auto accept to be used. The PIN could be entered by scanning a QR code.

EEBus SHIP recommends that a device can be reset to its original certificate using a factory reset (see [8] Section 12.2).

4.2.3 Secure communication channel

EEBus SHIP uses TLS to set up a secure communication channel (see the SHIP specification [8] section 9).

4.2.4 Logging

EEBus does not seem to support logging or status reporting mechanisms for security-related events. Logging functions should be explored, developed, and standardised.

4.2.5 Cryptography

EEBus SHIP specifies the cipher suites to be used for TLS (see the SHIP specification [8] section 9). The suites selected are according to best practices and meet the requirement CRY-1.

EEBus SHIP does use a SHA-1 hash for identifying nodes in the Subject Key Identifier. The SHA-1 hash algorithm is deprecated.

4.3 S2

The S2 standard, also referred to as EN 50491-12-2, is built as a semantic protocol only. The aim of this standard is to create dynamic coordination, or energy flexibility, between the Customer Energy Manager (CEM) and its FEIDs. The standard has no specifications on how the data should be transported or on any security-related aspects.

S2-ws-json is an open-source specification, which is currently still under development. This implementation allows the S2 standard to communicate over IP using web sockets. Implementations regarding security, such as secure authentication and encryption are not included.

Hence, in its current state it is not possible to meet the security requirements using the S2 protocol.

4.4 OCPP

The Open Charge Point Protocol (OCPP) is a protocol used for communication between a Charging Station Management System (CSMS) and a charging station. OCPP provides communication over WebSocket, which is secured through TLS.

Because OCPP is designed for direct communication between the CSMS and the charging station, it is difficult to securely integrate the HEMS into the architecture.

4.4.1 Access control

OCPP does not support role separation. So, to implement access control according to the requirement ACM1, the connector should only implement the functions that are needed for the HEMS.

For this access control model to work, the parallel control by the CSMS and EMS topology should be used, as defined in Section 9.6 of the OCPP Architecture & Topology document [9]. The charging station would set up separate OCPP connections to the CSMS and the HEMS (or EMS in the diagram). The functionality on the HEMS would be limited to the smart charging uses cases in OCPP (section K in the OCPP specification [10]).

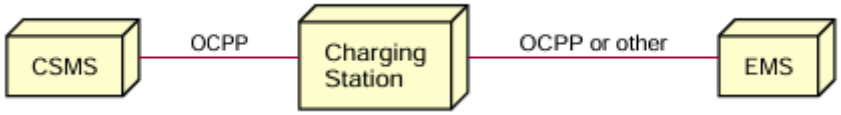

Figure 2: Parallel control by CSMS and EMS topology.

It would not be recommended to use a topology where the HEMS acts as a local controller or man-in-the middle (see Section 9.3 and 9.4 of [9]).

In the local controller topology, the controller would act as the CSMS to the charging station. Hence, it needs access to the full functionality that OCPP provides. If the HEMS were compromised, attackers could abuse the privileged access that the local controller has. They could for instance try to send messages through the local controller to change the keys on the charging station or change security settings.

Similarly, if the HEMS acts as a man-in-the-middle, the HEMS itself would be seen as the CSMS by the charging station, and hence would need privileged access.

The limitations of using a proxy could potentially be overcome by using signed messages (see Section 7 in the OCPP JSON over WebSocket implementation [11]). Critical messages from the CSMS could be signed by a private key known only to the CSMS, so that the charging station knows they are not coming from the HEMS. The charging station would reject critical messages if they were not signed. Such a use of signed messages would however require major changes to the charging station and CSMS, and does not seem desirable.

4.4.2 Authentication and pairing

OCPP does not support any mechanism for pairing the charging station with the HEMS. A new mechanism would have to be developed and standardized.

Once the pairing has been completed, OCPP can support mutual authentication through security profile 2 (TLS with basic authentication) or 2 (TLS with client-side certificates), see [10]. Which profile is used depends on how pairing will be implemented. Both profiles meet the authentication requirement AUM-2-B. For interoperability, the connectors must support the same profile on the HEMS and FEID side.

The connectors should not allow communication using profile 1, as it does not support authentication.

4.4.3 Secure communication channel

OCPP supports a secure communication channel by using TLS. To use TLS, the connectors should implement security profile 2 (TLS with basic authentication) or 2 (TLS with client-side certificates), see [10]. Both profiles meet the secure communication requirements.

The connectors should not allow communication using profile 1, as it does not support secure communication.

4.4.4 Logging

OCPP supports requirements for security logging, which are in line with requirement LGM-1.

4.4.5 Cryptography

OCPP requires that the cryptographic algorithms recommended by the German BSI are used. Requirements are also included on the length of cryptographic keys. So, if connector follows the OCPP standard, they will meet requirement CRY-1.

Annex: Mapping to RED requirements

This section provides a mapping between the requirements in Section 3 and the harmonized standard EN 18031 developed for the Radio Equipment Directive (RED) delegated act on cybersecurity. From 1 August 2025, radio equipment should meet the requirements in the EN 18031 standard. Hence, they are a good basis for cybersecurity requirements for the connectors.

It is expected that EN 18031 will also be the basis for future harmonized standards that will be developed for the Cyber Resilience Act, which will apply from December 2027.

Only parts 1 and 2 of the EN 18031 standard are considered. Part 1 applies to all internet-connected radio devices, and part 2 applies to devices processing personal data. The HEMS and FEIDs process power measurements, which can in some cases be personal data. Part 3 of EN 18031 applies to devices performing financial transactions and hence is not considered here.

Table 2: Coverage of the requirements in the EN 18031 harmonized standard for the radio equipment directive by the connector requirements.

EN 18031-1 requirement	**Connector requirements coverage**
[ACM-1] Applicability of access control mechanisms	*Fully covered* – Requirements [ACM-1] specifies that access control is applicable for all functions on the connector
[ACM-2] Appropriate access control mechanisms	*Fully covered* – Requirement [ACM-2] defines the appropriateness of access control
[ACM-3] Default access control for children in toys	*Not applicable* – Only applies to children's toys.
[ACM-4] Default access control to children's privacy assets for toys and childcare equipment	*Not applicable* – Only applies to children's toys and childcare equipment.
[ACM-5] Parental/Guardian access controls for children in toys	*Not applicable* – Only applies to children's toys.
[ACM-6] Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys	*Not applicable* – Only applies to children's toys.
[AUM-1-1] Requirement network interface	*Fully covered* – The requirements [AUM-2-A/B/C] also cover the applicability of access control

[AUM-1-2] Requirement user interface	*Not applicable* – All access is over network interfaces and is covered by [AUM-1-1].
[AUM-2] Appropriate authentication mechanisms	*Fully covered* – Requirements [AUM-2-A/B] define the authentication during and after pairing.
[AUM-3] Authenticator validation	*Fully covered* – [AUM-3] specifically covers the validation of certificates, as these are the most commonly used authentication method.
[AUM-4] Changing authenticators	*Fully covered* – [AUM-4] allows to renew the pairing to change the authenticators used after pairing.
[AUM-5-1] Requirement for factory default passwords	*Covered through documentation* – Developers are required to provide documentation on securely initializing passwords and other credentials according to [AUM-5/6]. The actual initialization of passwords is implemented by the HEMS or FEID developer.
[AUM-5-2] Requirement for non-factory default passwords	*Covered through documentation* – Developers are required to provide documentation on securely initializing passwords and other credentials according to [AUM-5/6]. The actual initialization of passwords is implemented by the HEMS or FEID developer.
[AUM-6] Brute force protection	*Covered through documentation* – Developers are required to provide documentation on securely initializing passwords and other credentials according to [AUM-5/6]. The actual initialization of passwords is implemented by the HEMS or FEID developer.
[SUM-1] Applicability of update mechanisms	*Not applicable* – The connectors are not involved in performing firmware updates.
[SUM-2] Secure updates	*Not applicable* – The connectors are not involved in performing firmware updates.
[SUM-3] Automated updates	*Not applicable* – The connectors are not involved in performing firmware updates.
[SSM-1] Applicability of secure storage mechanisms	*Not applicable* – Secure storage should be implemented by the developer of the HEMS or FEID.

[SSM-2] Appropriate integrity protection for secure storage mechanisms	*Not applicable* – Secure storage should be implemented by the developer of the HEMS or FEID.
[SSM-3] Appropriate confidentiality protection for secure storage mechanisms	*Not applicable* – Secure storage should be implemented by the developer of the HEMS or FEID.
[SCM-1] Applicability of secure communication mechanisms	*Fully covered* – See requirement [SCM-1].
[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms	*Fully covered* – See requirement [SCM-2].
[SCM-3] Appropriate confidentiality protection for secure communication mechanisms	*Fully covered* – See requirement [SCM-3].
[SCM-4] Appropriate replay protection for secure communication mechanisms	*Fully covered* – See requirement [SCM-4].
[RLM-1] Applicability and appropriateness of resilience mechanisms	*Partially covered* – A requirement is included to perform robustness testing on the connector ([RLM-1]) to avoid resilience issues in the application layer. Lower layer resilience issues must be mitigated in the HEMS or FEID itself.
[NMM-1] Applicability and appropriateness of network monitoring mechanisms	*Not applicable* – The connector is not considered network equipment under the definitions in EN 18031.
[TCM-1] Applicability of and appropriate traffic control mechanisms	*Not applicable* – The connector is not considered network equipment under the definitions in EN 18031.
[LGM-1] Applicability of logging mechanisms	*Fully covered* – See requirement [LGM-1].
[LGM-2] Persistent storage of log data	*Not applicable* –*S*torage of the logs should be implemented on the HEMS or FEID.
[LGM-3] Minimum number of persistently stored events	*Not applicable* –*S*torage of the logs should be implemented on the HEMS or FEID.

[LGM-4] Time-related information of persistently stored log data	*Not applicable* –*S*torage of the logs should be implemented on the HEMS or FEID.
[DLM-1] Applicability of deletion mechanisms	*Not applicable* – Should be implemented on the HEMS or FEID, not in the connector.
[UNM-1] Applicability of user notification mechanisms	*Not applicable* – Should be implemented on the HEMS or FEID, not in the connector.
[UNM-2] Appropriate user notification content	*Not applicable* – Should be implemented on the HEMS or FEID, not in the connector.
[CCK-1] Appropriate CCKs	*Partially covered* – Keys used by the connector are required to have at least an 112-bit strength, so that they must be initialized by the HEMS or FEID to this strength.
[CCK-2] CCK generation mechanisms	*Covered through documentation* – The security documentation is required to have guidance on initializing cryptographic keys securely ([CCK-2/3]).
[CCK-3] Preventing static default values for preinstalled CCKs	*Covered through documentation* – The security documentation is required to have guidance on initializing cryptographic keys securely ([CCK-2/3]).
[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities	*Fully covered* – The developer is required to deliver the connector without known vulnerabilities through requirement [GEC-1-A]. Verifications for vulnerabilities are included in requirements [GEC-1-B] and [GEC-1-C].
[GEC-2] Limit exposure of services via related network interfaces	*Covered through documentation* – The security documentation includes the network services that are exposed by the connector and how these should be hardened. See requirement [GEC-2/4]
[GEC-3] Configuration of optional services and the related exposed network interfaces	*Covered through documentation* – The security documentation includes the network services that are exposed by the connector and how these should be hardened. See requirement [GEC-2/4]
[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces	*Covered through documentation* – The security documentation includes the network services that are exposed by the connector and how

	these should be hardened. See requirement [GEC-2/4]
[GEC-5] No unnecessary external interfaces	*Partially covered* – The security documentation includes the network services that are exposed by the connector and how these should be hardened. See requirement [GEC-2/4]
[GEC-6] Input validation	*Partially covered* – Input validation is covered in the secure development requirements. See requirement [GEC-6].
[CRY-1] Best practice cryptography	*Fully covered* – Covered by requirement [CRY-1].

References

[1] ENISA, "EUCC Scheme Guidelines on cryptography - Agreed Cryptographic Mechanisms, Version 2, May 2025," 2025.

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

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

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

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

[6] Connectivity Standards Alliance, "Matter Specification, Version 1.4.1," 2025.

[7] Silicon Labs, "Matter Security (version 2.6.1)," 2025. [Online]. Available: https://docs.silabs.com/matter/2.6.1/matter-fundamentals-security/.

[8] EEBus Initiative, "EEBus Technical Specification - Smart Home IP, Version 1.0.1," 2019.

[9] Open Charge Alliance, "OCPP 2.1: Part 1 - Architecture & Topology, Edition 1," 2025.

[10] Open Charge Alliance, "OCPP 2.1: Part 2 - Specification, Edition 1," 2025.

[11] Open Charge Alliance, "OCPP 2.0.1: Part 4 - JSON over WebSockets implementation guide, Edition 1," 2025.

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