AN13645

Smart and secure EV Charging with NXP secure solutions

Rev. 1.0 — 28 November 2022 Application note

Document information

Information	Content
Keywords	EV, EVSE, secure element, ISO 15118, OCPP, EdgeLock, SE05x, A5000
Abstract	This document describes how NXP solutions such as EdgeLock SE05x/ A5000 and EdgeLock 2GO can be integrated in Electric Vehicle Supply Equipments (EVSEs) to meet the security requirements mandated by smart charging standards and protocols, such as ISO 15118 and OCPP, and by regional and local regulations.

Revision history

Revision history

Revision number	Date	Description
1.0	2022-11-28	Initial version

1 Introduction to smart charging

The adoption of Electric Vehicles (EVs) is rapidly growing sustained by improved battery performance, decreasing cost of components and government incentives. With government decisions, such as the EU only allowing new cars with zero C02 emissions from 2035 onwards, and more people choosing EVs over traditional vehicles with internal combustion engines, government agencies and private enterprises are moving quickly to deploy a robust network of publicly available *charging stations*, also known as Electric Vehicle Supply Equipments (EVSEs), in parking lots, along roadways, or wherever they are needed.

Far from being simple power outlets, EVSEs are expected to integrate with smart grids to optimize energy consumption and balance power distribution based on the current load of the network. On top of this, EVSEs should provide smart features and additional services to their users such as automated notifications, access to third-party services and a seamless *plug & charge* user experience for authentication, authorization and trustworthy billing. This requires EVSEs to communicate and exchange information with the different actors involved in the smart charging ecosystem such as EVs, Charging Point Operators (CPOs), Distribution System Operators (DSOs), eMobility Service Providers (eMSPs) and Original Equipment Manufacturers (OEMs).

Since EVSEs are the main entry point to the smart charging infrastructure, security is an essential requirement to build public trust, preserve user privacy, prevent unintended usage of the charging equipment and avoid disruption of critical components of the charging infrastructure. In fact, attackers can leverage insecure communication protocols or hardware and software vulnerabilities to gain unauthorized access to energy and customer information, manipulate billing data or even disrupt the operation of EVSEs and power grids. Implementing strong security countermeasures, supported by cryptographic credentials and protocols, is therefore an essential requirement to build a secure and reliable e-mobility infrastructure.

1.1 Overview of ISO 15118 and OCPP

Secure, interoperable standards and protocols are key to the success of smart charging. They must ensure interoperability between different EV manufacturers, smoothly integrate with the different entities that are involved in the smart charging ecosystem and be built on top of state-of-the-art, future-proof security that can withstand the requirements of present and future regulations. **Currently, the smart charging ecosystem is very fragmented** as several standards and protocols are being defined and are competing with one another to reach widespread market acceptance. Even so, some standards and protocols are slowly getting traction over similar competitors.

The ISO 15118 standard is gradually emerging as the leading standard for implementing secure, bidirectional communication between EVSEs and EVs. The standard offers the *Plug & Charge* feature which allows EVs to automatically identify and authorize themselves to a compatible EVSE on behalf of the driver. It also offers other advanced features, such as bidirectional charging (*V2G - Vehicle to Grid*) and wireless power transfer. All these features rely on strong cybersecurity provisions that have been designed to establish digital trust between the EV and the EVSE.

EVSEs must also be able to connect to a backend system responsible for managing the whole network of charging stations. **The Open Charging Point Protocol (OCPP) is an open source protocol promoted by the Open Charge Alliance (OCA) that can be used to connect EVSEs to a compatible Charging Station Monitoring System (CSMS)**. The protocol defines a set of messages, operations and use cases required to

manage a network of EVSEs. The latest version of the protocol integrates with ISO 15118 and defines a set of requirements for the secure operation of the system.

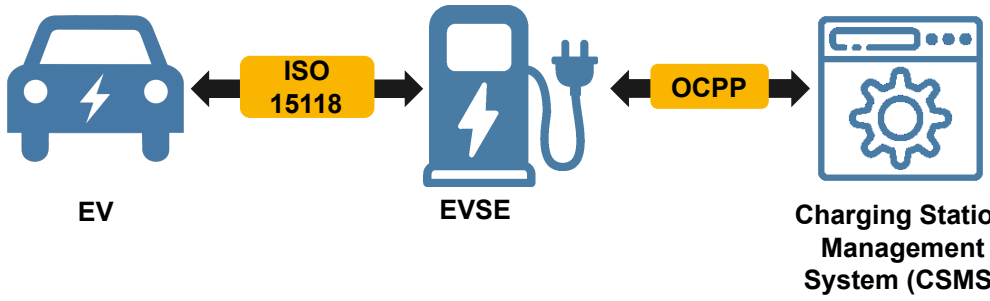

Figure 1. The ISO 15118 standard and OCPP protocol

1.2 Introducing NXP solutions for EVSEs

NXP provides scalable, flexible and secure solutions to develop future-proof EVSEs that fulfill the security and connectivity requirements mandated by ISO 15118 and OCPP and even go beyond that.

Enabling top-notch security on EVSEs is as easy as integrating the **NXP EdgeLock SE05x/A5000 secure element**: a ready-to-use SE solution tailor-made for the IoT that provides a secure, CC EAL 6+, AVA_VAN.5 certified tamper-resistant hardware to protect mission critical cryptographic credentials as well as a secure environment to offload cryptographic operations. EdgeLock SE05x/A5000 is pre-provisioned with keys and credentials in a highly secure and controlled environment, therefore relieving device manufacturers from setting up a complex and expensive Public Key Infrastructure (PKI). It also comes with a pre-installed applet and a Plug & Trust middleware package that ease the integration of the secure element in the device MCU/MPU.

To abstract the complexity of key and certificate management in secure elements and authenticators, NXP offers **EdgeLock 2GO**: a fully managed cloud platform that allows customers to create and manage secure objects, such as symmetric roots of trusts, key-pairs and certificates, which are then securely provisioned (either remotely or locally) into the secure elements of IoT devices. This gives customers the flexibility to securely manage the credentials of EVSEs already deployed in the field and to quickly and easily update them to meet new security requirements or react to security incidents.

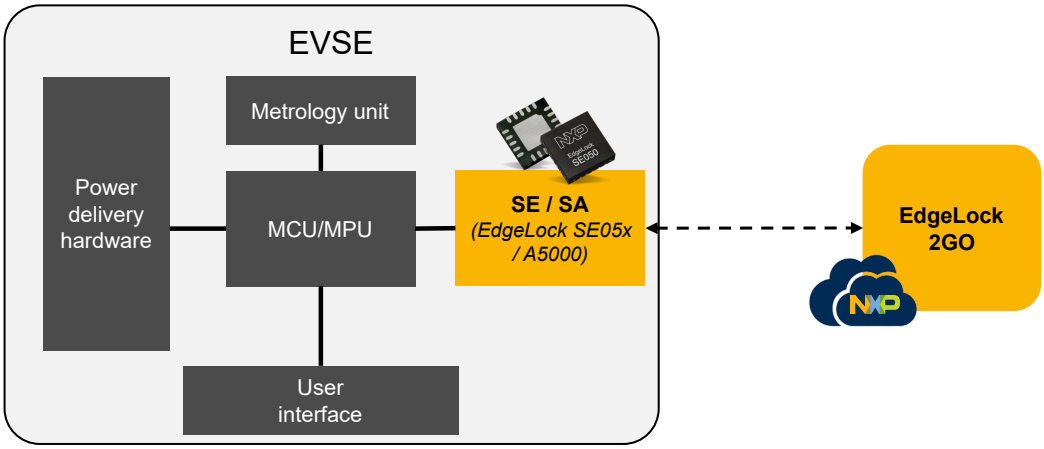

Figure 2. NXP secure solutions for smart charging stations

2 Architecture of a smart charging system

The smart charging infrastructure consists of several actors and components that communicate with one another with the objective of efficiently distributing energy resources and delivering to EV drivers the charging service and all other services they subscribed to. This requires smart charging systems to implement two primary interfaces: one for distributing electricity and another interface for control related to status, authorization, metering and billing. These interfaces are implemented by means of interoperable standards and protocols. The architecture of a typical smart charging system is depicted in Figure 3.

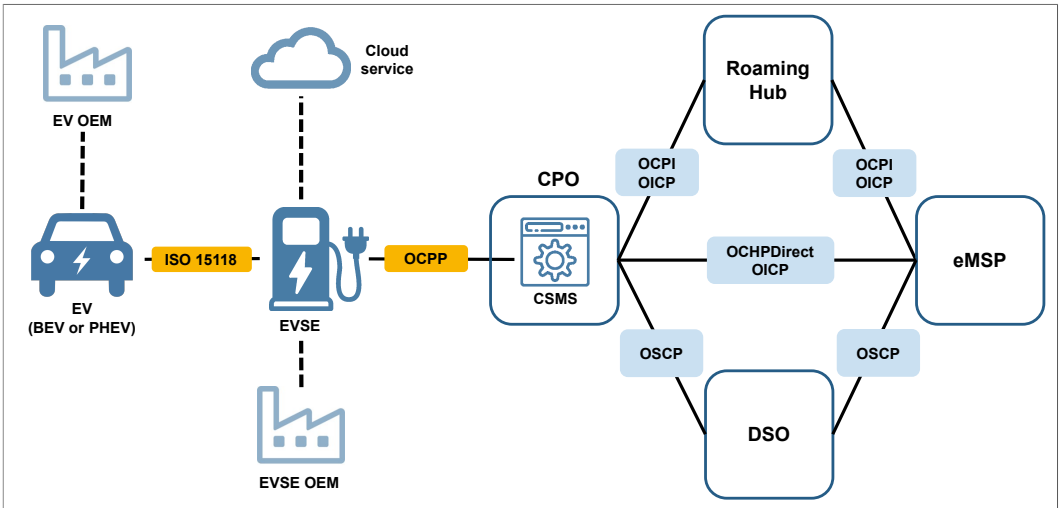

Figure 3. Smart charging system architecture

- **Electrical Vehicle (EV):** EVs integrate a battery and its corresponding Battery Management System (BMS). Through one or more power connectors integrated in the vehicle, users can charge the battery using private or public EVSEs. EVs can be divided in Battery Electric Vehicles (BEVs), i.e. fully electrical vehicles, or Plug-in Hybrid Electrical Vehicles (PHEV), i.e. vehicles integrating a smaller battery and a non-electrical power source such as gasoline.
- **Electrical Vehicle Supply Equipment (EVSE):** charging stations are the entry point through which EVs access the smart charging system. The EVSE communicates with the BMS of the EV so that the battery can be charged at the correct rate. An EVSE consists of a MCU/MPU that controls the device and a variety of interfaces, sensors and components such as a display, a metrology unit for energy measurement, NFC readers/bridges for maintenance purposes, POS terminals and discrete secure components (e.g. EdgeLock SE05x/A5000). Communication between the EVSE and the EV can be implemented through the ISO 15118 protocol (see Section 3.1). Depending on how it delivers power to the EV, an EVSE can be classified as:
  - **Alternate Current (AC) EVSE:** the most simple chargers, such as the ones typically used in residential areas, deliver AC power that comes from the grid to the EV's onboard AC-DC converter, which then feeds it into the car's battery. Since the converter is limited in size, AC charging stations are typically much slower. AC charging stations may onboard different types of plug connectors based on the market for which they are built. The most common connector is the SAE J1772 Type 1/Type 2 connector used in Europe and the US.
  - **Direct Current (DC) EVSE:** also known as fast chargers, DC charging stations embed an AC-DC converter and deliver DC power directly to the EV's battery.

DC charging allows the car to be charged significantly faster than AC charging. Currently, the most common charging stations are 50 kWh, but faster charging stations are emerging as well. AC charging stations may onboard different types of plug connectors based on the market for which they are built (e.g. CHAdeMO for Japan or CCS Type 1/Type 2 in the US and Europe).

- **Charging Point Operator (CPO):** this entity is responsible for managing a network of EVSEs through a cloud-based Charging Station Monitoring System (CSMS). A CSMS may provide a broad array of functionalities such as generating reports to monitor EV charging history, collecting statistics, running diagnostics on the EVSE network, scheduling charging based on time of the day and monitoring in real-time the usage of EVSEs. The most common way for EVSEs to communicate with a CSMS is through the OCPP protocol (see section Section 3.2).
- **Distribution System Operator (DSO):** this entity is responsible for distributing and managing energy from the generation sources to the final consumers. In a smart charging system, a DSO not only maintains and manage the power grid, but also actively performs tasks such as network congestion management and peak load management. The Open Smart Charging Protocol (OSCP) is an example of a protocol that can be used to provide to CPOs or eMSPs information about the available capacity of the network.
- **eMobility Service Providers (eMSPs):** these entities offer EV charging services, or other collateral services, to EV drivers. An eMSP may offer services from its own network of EVSEs or establish relationships with different EVSE networks to provide roaming services to its users. Before EV drivers can use public charging facilities, they must subscribe to the services offered by one or more eMSPs through pre-paid, post-paid or group plans. Communication between CPOs and eMSPs / roaming hubs can be implemented using protocols such as the Open Intercharge Protocol (OICP), Open Charge Point Interface (OCPI) and Open Clearing House Protocol (OCHP).
- **Cloud service(s):** EVSEs can optionally connect to proprietary cloud services, such as Microsoft Azure or AWS, to send/receive relevant data. Connection to the cloud can be established using a variety of protocols depending on the use case and desired level of security.
- **Original Equipment Manufacturers (OEMs):** EVs and EVSEs are manufactured by OEMs. OEMs take care of producing and distributing the equipment in the different markets in which they operate. In some cases, they also offer additional services after the equipment is purchased, e.g. periodical firmware updates.

2.1 Main security requirements for charging stations

Charging stations are one of the most vulnerable components of a smart charging infrastructure as they are often unmanned and located in areas where they can be easily accessed and manipulated. The following security considerations are essential to guarantee the secure operation of charging stations:

- **Authenticate EVs:** only authorized vehicles should be able to use the services offered by an EVSE. At the same time, EV should only accept to be charged by authorized charging stations. This requirement can be achieved by implementing the ISO 15118 standard which defines processes and requirements for the secure authentication of an EVSE to an EV (and vice versa) using cryptographic protocols (Transport Layer Security - TLS) and credentials (digital certificates). See Section 3.1.1 for an explanation of the ISO 15118 plug & charge feature. Detailed requirements related to this functionality are further discussed in Section 4.1.

- **Prevent fake or unauthorized chargers being installed:** fake or unauthorized chargers can be deployed in the field by malicious actors to steal energy or other sensitive data or to perform an attack towards the energy grid e.g., causing local blackouts. To avoid this, EVSEs must be provisioned with unique credentials that can be used to authenticate and remote attest the EVSE to the backend infrastructure and prove that the device is indeed authentic. This can be achieved by implementing the secure authentication and communication requirements of the OCPP protocol or by implementing remote attestation of the EVSE to implement a Zero Trust architecture within the grid. . Even so, the software running on the EVSE could be manipulated, modified or substituted by attackers and use provisioned credentials in an improper way. In this context, secure boot and secure firmware update ensure that software is original when the device is booted or when a new software is uploaded to the EVSE. The OCPP protocol defines a secure process for retrieving and installing firmware updates as described in Section 4.2.3. How to strengthen the process using EdgeLock SE05x/A5000 is further discussed in Section 5.
- **Implement secure communication with the cloud:** the EVSE needs to communicate securely with cloud services (e.g. the CSMS) over potentially insecure networks such as the internet. It is therefore essential that data is properly encrypted before it is sent over the network, so only intended recipients can read the data. To meet this requirement, both the ISO 15118 standard and OCPP protocol make use of Transport Layer Security (TLS) for (mutual) authentication and data encryption as discussed in Section 4.1.3 (ISO 15118) and Section 4.2.2 (OCPP).
- **Authenticate transactions:** charging stations typically generate many transactions, for example to report energy usage to the backend which then bills the user according to the energy consumed. Transaction undeniability of an EVSE is therefore essential to prevent attackers from generating fake transactions and taking advantage of the charging infrastructure. Digital cryptographic signatures are the key enabler to ensure the authenticity of transactions: by using a device-unique private key securely stored in the EVSE, the device can sign transactions that can be later verified by any third party system using the associated public key. This is for example a requirement of the German Eichrecht regulation described in Section 3.3.

3 Standards, protocols and regulations for charging stations

This section provides a brief overview of the standards, protocols and regulations that will be covered in this document:

- The ISO 15118 standard is described in Section 3.1. The standard covers EV to EVSE communication.
- The OCPP protocol is described in Section 3.2. The protocol covers EVSE to CSMS communication.
  ***Note**: there are other existing protocols such as IEC63110. However, this document focus on OCPP.*
- Local and regional regulations for EVSEs are covered in Section 3.3.

3.1 The ISO 15118 standard

The ISO 15118 standard consists of several standard documents defining different aspects of a Vehicle to Grid (V2G) communication interface for bi-directional charging/discharging of EVs. Currently, the ISO 15118 is organized into 7 parts:

- **ISO 15118-1:** it specifies terms and definitions, general requirements and use cases for conductive and wireless high-level communication between the EV and the EVSE.
  ***Note:** in ISO 15118 EVSEs are referred to as Supply Equipment Communication Controllers (SECCs). Throughout this document the two terms will be used interchangeably.*
- **ISO 15118-2 (20):** this is the core part of the standard as it specifies the actual application layer messages and parameters that are exchanged between EVs and EVSEs. Based on this part, the use cases defined in ISO 15118-1 can be implemented. In this part of the standard, two types of application messages are defined: *SECC Discovery Protocol (SDP) messages*, which are used to exchange connection information, and *V2G messages*, which handle all other communication needs, from starting a session and entering a charging loop to terminating a session. Before they are sent, messages are compressed using the *Efficient XML Interface (EXI)* format and additional control headers are added by the *Vehicle-to-Grid Transport Protocol (V2GTP)*. Finally, messages are routed and delivered through standard IP-based protocols such as IP, UDP (for *SDP messages*) and TCP (for *V2G messages*) operating at the network and transport layer.
  ***Note:** a new version of the standard (ISO 15118-20) has been introduced for the second generation of network and application layer. See Section 4.1.4 for more information.*
- **ISO 15118-3 & ISO 15118-8:** these two parts specify respectively the requirements of the physical and data link layer for wired charging and for wireless charging.
- **ISO 15118-4, ISO 15118-5 & ISO 15118-9:** these parts of the standards define conformance tests for, respectively, the network and application protocol, the wired physical and data link layer and the wireless physical and data link layer.

Figure 4 shows the ISO 15118 protocol stack and how the different parts of the standard map to it.

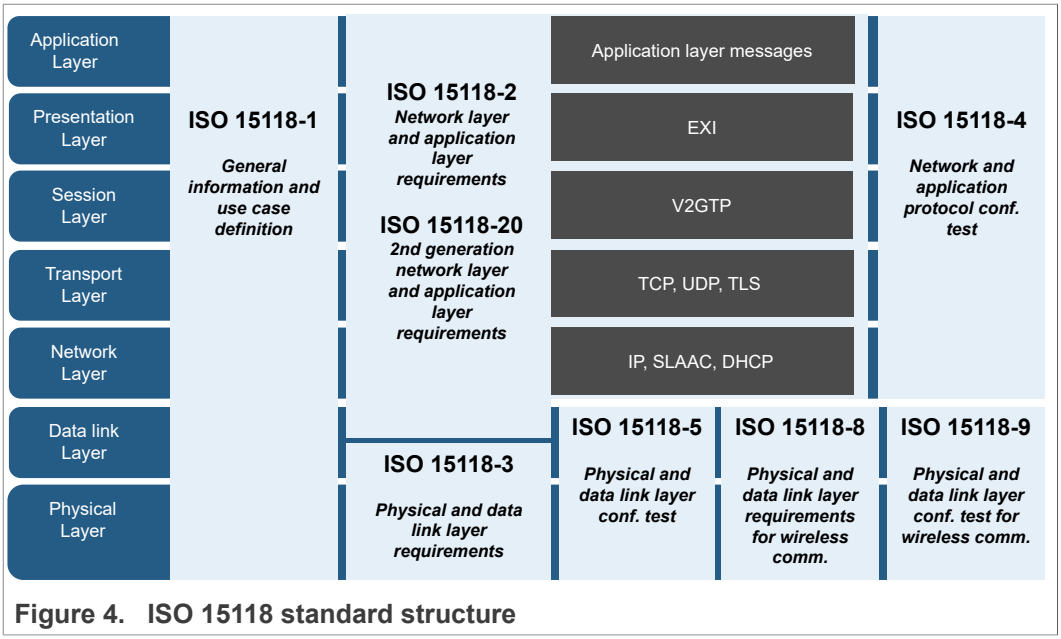

Figure 4. ISO 15118 standard structure

3.1.1 The ISO 15118 Plug & Charge features

One of the most important and anticipated features of ISO 15118 is *Plug & Charge* which provides a way for authenticating and authorizing EVs for a charging session using only digital certificates and signatures. Figure 5 provides a simplified representation of how *Plug & Charge* works in ISO 15118-2.

1. For *Plug & Charge* to work, charging stations must be provisioned with a set of cryptographic credentials (key pair) and their associated digital certificate (*CS certificate*) signed by a chain of publicly trusted Certificate Authorities (CAs). At the top of the chain resides a root CA (e.g. *V2G Root CA 1*) that must be trusted both by the EVSE and the EV.
   Note: *several certificates, signed by different V2G Root CAs, can be stored in the EVSE.*
   Note: *for PKI best security practice, it is recommended to diversify the credentials and make them unique.*
2. Upon connection of the EV to the EVSE, a TLS handshake is initiated between the two entities. First, the EV sends to the EVSE a list of trusted CA certificates (e.g., including *V2G Root CA 1* whose certificate must be pre-provisioned in the EV).
3. The EVSE selects a valid certificate (e.g., the *CS certificate* signed by *V2G Root CA 1*) and sends it to the EV together with the whole certificate chain. The EV verifies the signature of each certificate in the chain, from the *CS certificate* all the way up to the *V2G Root CA certificate*, and authenticates the EVSE. If all certificates are valid, and upon successful EVSE authentication, then a secure TLS connection is established.
   Note: *ISO 15118-20 mandates mutual authentication between the EV and the EVSE. If ISO 15118-20 is used, when a TLS channel is established the EVSE must present a valid certificate to the EV and the EV must provide a valid certificate to the EVSE.*
4. Before the EVSE permits the EV to charge its battery, the EV needs to present a valid *contract certificate*. The contract certificate is released by the eMSP when the user subscribes to the charging service. The contract certificate is linked to the user

billing account via a unique identifier, also known as the *E-Mobility Account Identifier (EMAID)* and is signed by the *eMSP root CA*.
Note: *refer to the ISO 15118 standard to learn how contract certificates can be provisioned in EVs through charging stations.*
Note: *since the EMAID contains privacy-related data, the EVSE shall handle this data taking into consideration privacy related regulations e.g. GDPR.*

5. The EVSE verifies the validity of the contract certificate using the *eMSP root CA* which is either pre-provisioned in the EVSE or is retrieved on-the-fly from the eMSP. If the contract certificate is valid, the EV is authorized and the charging process is started.

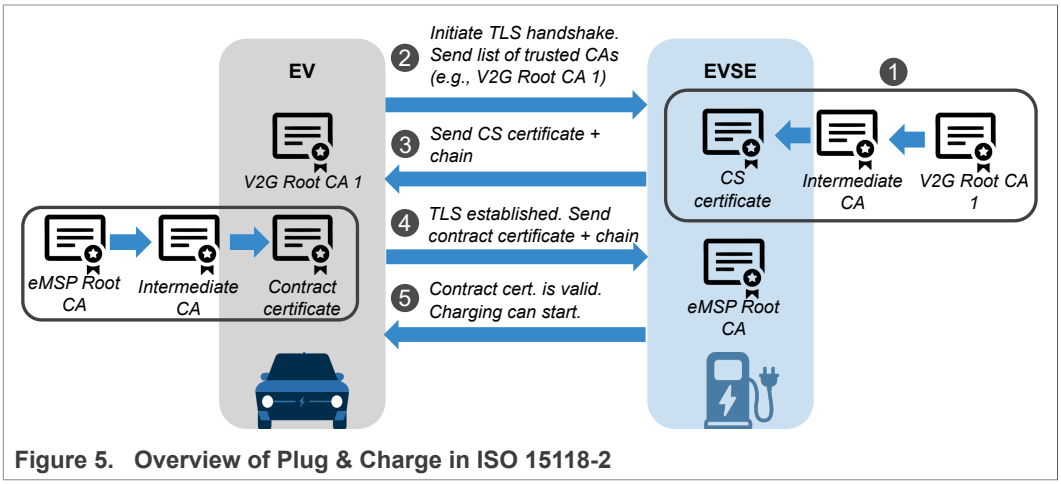

Figure 5. Overview of Plug & Charge in ISO 15118-2

3.2 The OCPP protocol

The Open Charge Point Protocol (OCPP) is an open-source communication protocol that is being developed by the Open Charge Alliance: a global consortium of public and private electric vehicle infrastructure companies. Since its inception in 2009, OCPP has become a de-facto standard enabling transparent communication between EVSEs and the CSMS. Through the message data structures defined by OCPP, it is possible to handle operations such as starting/stopping charging sessions, manage chargers, initiate firmware upgrades, and many others. Two main version of the protocol have been released:

- **OCPP 1.6:** this is the most popular version of the protocol for commercial deployments. Compared to earlier versions, version 1.6 introduced support for JSON over WebSockets alongside SOAP. Moreover, it introduced features such as smart charging, the ability to set restrictions on an individual charger and authorized local lists, to determine who is allowed to charge on each charging unit. Even though it is widely used, this OCPP version defines very limited security provisions which make it vulnerable to cyberattacks.
  Note: *OCPP 1.6-J has been introduced to port some of the security enhancements of OCPP 2.0.*
- **OCPP 2.0:** this version of the protocol, released in 2020, offers improved smart charging capabilities, new device management functionalities, improved transaction handling, reduced data usage, and, most importantly, a set of security additions which make the protocol more resistant to cyberattacks. The security extension includes secure firmware updates, security logging and event notifications and secure authentication and communication over Tranport Layer Security (TLS). Version 2.0 also introduces native support for vehicle-to-grid operations and ISO 15118-2 standard for

Plug & Charge. Since substantial changes have been introduced to the protocol, OCPP 2.0 is not backward compatible with OCPP 1.6.

The protocol consists of several functional blocks, each one defining a set of use cases, their associated requirements and the messages that need to be exchanged to correctly implement each use case. As of version 2.0.1, the protocol consists of 16 functional blocks, with more than 100 use cases covered. Functional blocks defined in OCPP 2.0.1 are listed in Table 1.

Table 1. OCPP 2.0.1 functional blocks

Functional block	Description
Security	Describes the security requirements for the OCPP protocol.
Provisioning	Describes all the functionalities that help a CPO provision their EVSE, allowing them on their network and retrieving configuration information from these charging stations.
Authorization	Describes different ways of authorizing a user, online and/or offline.
Local Authorization list management	The Local Authorization List is a list of identifiers that can be synchronized with the CSMS. This functional block is for enabling the CSMS to synchronize the list.
Transactions	Describes the OCPP transaction-related functionalities.
Remote control	Describes how to remotely control the EVSE, e.g. for unlocking a connector.
Availability	Specifies how the EVSE can inform the CSMS of its current availability for starting new transactions.
Reservation	The reservation functionality enables an EV Driver to make a reservation of an EVSE.
Tariff & Cost	Provides tariff and cost information to an EV Driver, when an EVSE is capable of showing this on a display.
Meter values	Enables an EVSE to send periodic metering data relating to transactions.
Smart Charging	Describes all the functionalities that enable the CPO (or a third party) to influence the charging current/power transferred during a transaction, or set limits to the amount of current/power an EVSE can draw from the grid.
Firmware management	Describes the functionality that enables a CPO to update the firmware of an EVSE.
15118 certificate management	Supports operations required for implementing the Plug & Charge feature (e.g. install / update certificates) as defined in ISO 15118-2.
Diagnostics	Enables remote diagnostics of problems that an EVSE is experiencing.
Display message	Enables a CPO to display a message or a cycle of messages on an EVSE.
Data transfer	Describes the functionality that enables parties to extend existing commands with custom attributes or add new custom commands to OCPP.

3.3 Compliance with local regulations

As EVs and public EVSEs become more and more widespread, governments and regulatory agencies are moving towards introducing laws and regulations that protect consumers from frauds and other abuses. These regulations might force OEMs and CPOs to implement in charging stations certain standards and protocols (e.g. ISO 15118 standard, GDPR for privacy), some of their security provisions or even stricter or different security requirements and configurations.

An example of a regulation that has recently been put into force is the **Calibration Law for electrical vehicle chargers (or Eichrecht)** in the German market. The Eichrecht regulation requires all components of an EVSE involved in the collection and processing of energy to operate in a trustworthy and transparent way. To meet these requirements, charging stations must have a certified energy meter which correctly calibrates the energy used and physically displays this value to consumers. Moreover, the EVSE must sign and encrypt this information before sending it to the CPO, in order to prevent third parties from changing the data and to allow consumers to verify the correctness of the invoiced data, e.g. through a mobile application (*transparency app*) and a QR code shown on the EVSE display.

Figure 6 provides an overview of the Eichrecht requirements and the entities involved.

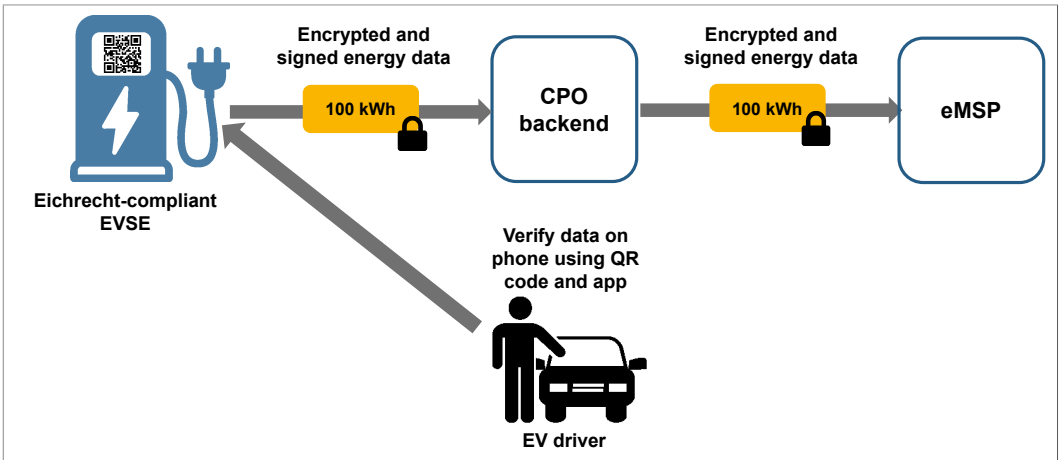

Figure 6. The German calibration law for EV chargers (Eichrecht)

4 Meet ISO 15118 and OCPP security requirements with NXP solutions

This section lists the security requirements mandated by ISO 15118 and OCPP that can be met by integrating in EVSEs NXP solutions such as EdgeLock SE05x/A5000 and EdgeLock 2GO. For this analysis, the ISO 15118-2:2014 standard and OCPP 2.0.1 protocol have been considered.

Note: *only security requirements that can be fully or partially met with NXP solutions are listed in this section. For a complete list of requirements, including software and hardware requirements, please refer to the standard/protocol specification.*

4.1 ISO 15118-2 requirements

The security requirements of the ISO 15118-2 standard can be grouped in the following categories:

- Cryptographic keys, certificates and algorithms
- Cryptographic random number generation
- Secure TLS communication
- Overview of ISO 15118-20 new features and requirements

For each category, the specific requirements of the standard are listed and we will explain in detail how to meet these requirements by integrating NXP secure solutions in EVSEs. A list of relevant demos, examples, APIs and documentation will be provided to help meet the requirements using NXP secure solutions.

4.1.1 Cryptographic keys, certificates and algorithms

The security provisions of ISO 15118-2 rely on cryptographic credentials and digital certificates that are used to establish a secure, authenticated TLS channel between the EV and the EVSE and to sign transactions. These requirements set the security grounds for implementing the *Plug & Charge* functionality described in Section 3.1.1. Table 2 lists the requirements mandated by ISO 15118-2 for cryptographic keys, certificates and algorithms that must be used in the EVSE.

Table 2. ISO 15118-2 security requirements (cryptographic keys, certificates and algorithms)

Req. ID	Requirement definition
V2G2-005	Each V2G entity shall support Hash-operation SHA-256 (signature process) according to NIST FIPS PUB 180-4.
V2G2-006	Each V2G entity shall support signature operations using ECC-based elliptic curve (secp256r1) with signature algorithm ECDSA.
V2G2-007	The key length for ECC-based asymmetric cryptography each V2G entity uses shall be 256 bit.
V2G2-004	Each V2G entity shall use X.509v3 certificates.
V2G2-877	Each SECC shall support the storage of at least 10 V2G Root Certificates.
V2G2-010	The size of a certificate in DER-encoded form shall be not bigger than 800 bytes. For transmission, all certificates shall be DER encoded.
V2G2-122	Each V2G Entity shall have mechanisms to process ECDH key exchange.
V2G2-652, V2G2-653	Each V2G Entity shall be able to generate / verify XML signatures (see V2G2-006).

EdgeLock SE05x/A5000 allows EVSEs to securely generate and store unique credentials and certificates as secure objects inside its secure CC EAL6+ certified tamper-resistant

hardware. Cryptographic operations involving secure objects are always performed inside the SE protected environment using built-in cryptographic functions and algorithms implemented by the pre-installed IoT applet. **Supported algorithms include ECDSA and SHA-256 for signature operations** as required by *V2G2-005*, *V2G2-006*, *V2G2-652* and *V2G2-653*.

Moreover, private keys will never leave the boundaries of the SE. EdgeLock SE05x natively supports the generation of device-unique symmetric (AES, DES) and asymmetric keys (ECC, RSA) directly inside the secure environment provided by the SE. **ECC keys with high key length (up to 512 bits) and future-proof curves are natively supported, including *secp256r1* (*V2G2-006*) and the more secure *secp512r1* curve** which is mandated by the more recent ISO 15118-20 standard (see Section 4.1.4). **X.509 certificates can also be securely stored in the SE as binary files in DER format** (*V2G2-004, V2G2-877, V2G2-010*). All credentials stored in the SE can be protected against deletion and overwriting using policies. Through policies, credential usage can be limited as well (e.g. a key-pair can be used only for signing operations).

EdgeLock SE05x/A5000 is pre-provisioned for ease of use in NXP's secure facilities with a set of device-unique key-pairs, certificates and identifiers that can be used to establish the initial root of trust of the device. In case the OEM needs to provision different credentials than the ones securely provisioned by NXP, they can be manually created and injected in EdgeLock SE05x/A5000 or remotely generated and securely provisioned through the EdgeLock 2GO platform.

Table 3. NXP material: ISO 15118-2 cryptographic keys, certificates and algorithms

NXP material	Relevant content
Plug & Trust middleware APIs	• **Get handle of (pre)provisioned keys or objects:** sss_se05x_key_object_get_handle(), sss_key_store_get_key () • **Key creation:** sss_se05x_key_store_generate_key () • **Key import / injection:** sss_key_store_set_key(), Se05x_API_WriteECKey (), Se05x_API_WriteRSAKey () • **Read EdgeLock SE05x pre-injected UID:** Se05x_API_ReadObject(kSE05x_AppletResID_UNIQUE_ID)
Plug & Trust middleware demos and examples	• **Inject Certificate into SE example**: \simw-top\demos\se05x \se05x_InjectCertificate • **Get Certificate from the SE**: \simw-top\demos\se05x\se05x_GetCertificate • **Get Info example** (retrieve SE UID): \simw-top\demos\se05x\se05x_GetInfo • **Using policies for secure objects demo:** \simw-top\demos\se05x \se05x_policy • **EdgeLock 2GO Agent examples**:\simw-top\nxp_iot_agent\ex

4.1.2 Cryptographic random number generation

The cryptographic algorithms and protocols (including TLS) used by ISO 15118-2 require the generation of random initialization data or nonces for proof of possession. The requirements for cryptographic random number generation defined in ISO 15118-2 are listed in Table 4.

Table 4. ISO 15118-2 security requirements (cryptographic random number generation)

Req. ID	Requirement definition
V2G2-835	Whenever a V2G entity requires random numbers within this document, a state-of-the-art cryptographically secure random number generator shall be used.

EdgeLock SE05x/A5000 supports the generation of variable-length random numbers through the built-in **AIS20 NIST800-90A compliant Pseudo Random Number Generator (PRNG) with DRG.4 generation capabilities**. The PRNG works on top of EdgeLock SE05x/A5000 **True Random Number Generator (TRNG) compliant to AIS31 NIST800-90B class PTG.2**. More information on PRNG and TRNG can be found in EdgeLock SE05x Data Sheet and in EdgeLock A5000 Data Sheet.

Table 5. NXP material: ISO 15118-2 cryptographic random number generation

NXP material	Relevant content
Plug & Trust middleware APIs	• **Generate a random number:** sss_se05x_rng_get_random () • **Generate random data for TLS handshake:** Se05x_API_TLSGenerateRandom ()

4.1.3 Secure TLS communication

The TLS protocol is used in ISO 15118-2 to secure the communication between the EV and the EVSE and to authenticate the EVSE identity to the EV. Implementing TLS is mandatory to have access to the *Plug & Charge* functionality described in Section 3.1.1. Table 6 lists the requirements of ISO 15118-2 for the TLS channel.

Table 6. ISO 15118-2 security requirements (secure TLS communication)

Req. ID	Requirement definition
V2G2-631	Support of TLS is mandatory for the SECC for all identification modes except for identification mode EIM (External Identification Mode) in a trusted environment.
V2G2-067	Unilateral authentication with TLS v1.2 shall be supported by each V2G entity. The EV authenticates the SECC by verifying the SECC certificate chain provided from the SECC to the EV.
V2G2-068	The SECC shall always act as the TLS server component.
V2G2-602	The SECC shall support all cipher suites defined below: • TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 Additional cipher suites may be supported by any V2G entity.

EdgeLock SE05x/A5000 supports the cryptographic requirements and operations defined in Table 6. In fact both **ECDH / ECDHE algorithm for key agreement and ECDSA algorithm for digital signatures are supported**. AES symmetric keys of up to 256 bits are also supported and can be used in ECB, CBC, CTR, GCM and CCM operation modes for data encryption. Finally, the SHA-256 and SHA-384 algorithms are supported as well (EdgeLock SE05x additionally supports SHA-224 and SHA-512). To simplify even more the integration of TLS, **the Plug & Trust middleware provides an mbedTLS ALT implementation** which allows the mbedTLS stack to use the secure element to perform the crypto operations that are part of the TLS handshake between client and server.

The following NXP material can be used as a starting point to meet the requirements listed above:

Table 7. NXP material: ISO 15118-2 secure TLS communication

NXP material	Relevant content
Plug & Trust middleware APIs	• **Perform TLS handshake:** Se05x_API_TLSCalculatePreMasterSecret (), Se05x_API_TLSGenerateRandom (), Se05x_API_TLSPerformPRF()

Table 7. NXP material: ISO 15118-2 secure TLS communication...*continued*

NXP material	Relevant content
Plug & Trust middleware demos and examples	• **TLS Client example**: \simw-top\demos\linux\tls_client
Application notes	• AN12400 EdgeLock SE05x for secure connection to OEM cloud

4.1.4 Overview of ISO 15118-20 new features and requirements

The ISO 15118-20 standard, released in 2022, defines new and updated requirements for the network and application layers. Since the standard has been recently released, its implementation and deployment is still in the very early phases: in fact, it is expected that it will take several years for entities participating in the smart charging ecosystem, including EVSE and EV manufacturers, to fully implement the new standard and be able to ship commercial products to the market. **Since the ISO 15118-20 is not backward compatible with ISO 15118-2, the two standards should be able to coexist for several years as EVSEs and EVs gradually transition to ISO 15118-20**. EVSEs should therefore support both versions of the standard for the time being and should be able to switch from one standard to the other based on the support provided by the EV.

The main changes in the security provisions of ISO 15118-20 compared to ISO 15118-2 are outlined below:

- **Stronger cryptography:** ISO 15118-20 mandates the usage of stronger cryptographic keys and algorithms (e.g. for establishing the secure TLS channel and for signature operations). In particular, the minimum key length for ECC-based asymmetric cryptography is now 521 bits. Moreover, stronger algorithms must be supported, such as SHA-512 and ECDSA with *secp521r1* curve for signature operations. EdgeLock SE05x already supports the secure generation and storage of 521 bits ECC keys using several curves, including *secp521r1*. Moreover, EdgeLock SE05x supports ECDSA and SHA-512 algorithms for signature generation and verification.
- **Mutual TLS:** contrary to ISO 15118-2 where only the EVSE authenticates with the EV, in ISO 15118-20 a mutual TLS authentication must be performed, i.e. the EV must authenticate the EVSE and the EVSE must authenticate the EV. This is done using credentials and certificates that are securely injected and stored in both the EV and the EVSE.
- **TLS version:** TLS is mandatory for all communication modes and the minimum supported TLS version is version 1.3. As such, supported ciphersuites have been updated to support stronger algorithms (e.g. *TLS_AES_256_GCM_SHA384*) as defined in the latest version of the TLS standard. EdgeLock SE05x already supports all the required crypto operations that are needed to establish a secure, mutually authenticated TLS channel using ECDHE, AES in GCM mode using 256 bits session keys and SHA-384.
- **Higher cryptographic agility:** the standard defines security provisions that mandate EVSEs and EVs to switch to more robust cryptographic algorithms and cipher suites in case recommended algorithms are compromised or become obsolete.
- **New certificate requirements:** X.509 certificates can now have a bigger size (up to 1600 bytes instead of 800 bytes) and can be cross-signed, so as to reduce the number of certificates that needs to be provisioned in EVSEs/EVs.

4.2 OCPP 2.0.1 requirements

The security requirements of the OCPP 2.0.1 protocol can be grouped in the following categories:

- Cryptographic keys, certificates and algorithms
- Secure authentication and communication requirements
- Secure firmware update requirements

For each category, the specific requirements of the protocol are listed and we will explain in detail how to meet these requirements by integrating NXP secure solutions in EVSEs. A list of relevant demos, examples, APIs and documentation will be provided to help meet the requirements using NXP secure solutions.

4.2.1 Cryptographic keys, certificates and algorithms

The OCPP protocol security provisions rely on unique cryptographic credentials and digital certificates that are used to establish a secure, authenticated TLS session between the EVSE and the CSMS and to decrypt firmware updates and verify their signature. Table 8 lists the requirements / recommendations mandated by OCPP for credentials and certificates that are installed in EVSEs.

Table 8. OCPP requirements: credential installation and certificate properties

Req. ID	Requirement definition
A00.FR.427	A unique Charging Station certificate SHALL be used for each Charging Station.
A00.FR.501, A00.FR.502, A00.FR.503	All certificates SHALL use a private key that provides security equivalent to a symmetric key of at least 112 bits (RSA - 2048 bits, ECC - 224 bits)
A00.FR.505	For signing by the certificate authority RSA-PSS, or ECDSA SHOULD be used.
A00.FR.508, A00.FR.511	All certificates SHALL include a serial number. For the Charging Station certificate, the subject field SHALL contain a CN (commonName) RDN which consists of the unique serial number of the Charging Station.
A00.FR.801, A00.FR.802	It is RECOMMENDED that the manufacturer initializes the Charging Station with unique credentials during manufacturing. The credentials SHOULD be generated using a cryptographic random number generator, and installed in a secure environment.
A02.FR.01	A key update SHOULD be performed after installation of the Charging Station, to change the key from the one initially provisioned by the manufacturer (possibly a default key).
A02.FR.05	The private key generated by the Charging Station during the key update process SHALL NOT leave the Charging Station at any time, and SHALL NOT be readable via OCPP or any other (remote) communication connection.

Meet A00.FR.427, A00.FR.501, A00.FR.502, A00.FR.503: EdgeLock SE05x/A5000 allows EVSEs to securely generate and store credentials and certificates as secure objects inside its secure tamper-resistant hardware. Cryptographic operations involving secure objects are always performed inside the SE protected environment using built-in cryptographic functions and algorithms provided by the pre-installed EdgeLock SE05x/ A5000 IoT applet. Moreover, private keys will never leave the boundaries of the SE. EdgeLock SE05x natively supports the generation of device-unique symmetric (AES, DES) and asymmetric keys (ECC, RSA) directly inside the secure environment provided by the SE:

- EdgeLock SE05x supports RSA keys of up to 4096 bits;
- EdgeLock SE05x supports ECC keys with future proof curves and high key length: Brainpool (160 to 512 bits), NIST (192 to 521 bits), Edwards (curve 25519 and curve 448), Montgomery (curve 25519 and curve 448) and Koblitz (160 to 256 bits).
- X.509 certificates associated to generated credentials can also be securely stored in the SE as binary files in DER format.

All credentials stored in the SE can be protected against deletion and overwriting using policies. Through policies, credential usage can be limited as well (e.g. a key-pair can be used only for signing operations).

Meet A00.FR.427, A00.FR.801 and A00.FR.802: EdgeLock SE05x/A5000 is pre-provisioned for ease of use in NXP's secure facilities with a set of device-unique key-pairs, certificates and identifiers that can be used to establish the initial root of trust of the device. In case the OEM needs to provision different credentials than the ones securely provisioned by NXP, those can be manually created and injected in EdgeLock SE05x/ A5000 or remotely generated and securely provisioned through the EdgeLock 2GO platform.

Note: *different variants of EdgeLock SE05x might be pre-provisioned with a different set of credentials.*

Meet A00.FR.508, A00.FR.511: EdgeLock SE05x/A5000 is pre-injected in NXP's secure facilities with a device-unique, read-only 7-byte UID that can be used to identify the EVSE. A custom identifier can also be injected in EdgeLock SE05x/A5000 and protected against deletion and overwriting using the appropriate policies.

Meet A00.FR.505, A02.FR.01, A02.FR.05: the EdgeLock 2GO platform allows users to generate asymmetric key pairs (ECC or RSA) and their associated certificate and provision them securely into the SE of the device from the cloud. Client certificates generated by EdgeLock 2GO can be signed by the NXP root CA using the ECDSA algorithm. Alternatively, it is also possible to use a custom root CA. In both cases, keys are securely generated by EdgeLock 2GO and stored in EdgeLock 2GO secure hardware storage so users don't have to manage their own PKI. By integrating EdgeLock 2GO in EVSEs it becomes easy to rotate keys and certificates, for example to react to a security incident or to keep up with evolving local regulations.

The following NXP material can be used as a starting point to meet the requirements listed above:

Table 9. NXP material: OCPP Cryptographic keys, certificates and algorithms

NXP material	Relevant content
Plug & Trust middleware APIs	• **Get handle of (pre)provisioned keys or objects:** sss_se05x_key_object_get_handle(), sss_key_store_get_key () • **Key creation:** sss_se05x_key_store_generate_key () • **Key import / injection:** sss_key_store_set_key(), Se05x_API_WriteECKey (), Se05x_API_WriteRSAKey () • **Read EdgeLock SE05x pre-injected UID:** Se05x_API_ReadObject(kSE05x_AppletResID_UNIQUE_ID)
Plug & Trust middleware demos and examples	• **Inject Certificate into SE example**: \simw-top\demos\se05x \se05x_InjectCertificate • **Get Certificate from the SE**: \simw-top\demos\se05x\se05x_GetCertificate • **Get Info example** (retrieve SE UID): \simw-top\demos\se05x\se05x_GetInfo • **Using policies for secure objects demo:** \simw-top\demos\se05x \se05x_policy • **EdgeLock 2GO Agent examples**:\simw-top\nxp_iot_agent\ex

4.2.2 Secure TLS communication

The OCPP protocol defines three security profiles for establishing a secure (authenticated) channel between the EVSE and the CSMS as shown in Table 10. Even though the first two security profiles provide basic authentication mechanisms, only the third profile (TLS with Client Side Certificates) guarantees the establishment of a truly secure, mutually authenticated channel between the EVSE and the CSMS.

Table 10. Overview of OCPP security profiles

Profile	EVSE authentication	CSMS authentication	Communication security
1. Unsecured Transport with Basic Authentication	HTTP Basic authentication	-	-
2. TLS with Basic Authentication	HTTP Basic authentication	TLS authentication using certificate	TLS
3. TLS with Client Side Certificates	TLS authentication using certificate	TLS authentication using certificate	TLS

Integrating EdgeLock SE05x/A5000 in EVSEs allows customers to implement all the security requirements mandated by security profile 3 (TLS with Client Side Certificates).

Table 11. OCPP secure authentication & communication requirements (Profile 3)

Req. ID	Requirement definition
A00.FR.401	The Charging Station SHALL authenticate itself to the CSMS using the Charging Station certificate.
A00.FR.402	The Charging Station certificate SHALL be used as a TLS client side certificate
A00.FR.415	The communication channel SHALL be secured using Transport Layer Security (TLS)
A00.FR.416	The Charging Station and CSMS SHALL only use TLS v1.2 or above.
A00.FR.421, A00.FR.422	The Charging Station SHALL support at least one of these cipher suites: • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 and TLS_RSA_WITH_AES_256_GCM_SHA384 ***Note**: TLS_RSA does not support forward secrecy, therefore TLS_ECDHE is RECOMMENDED.*

EdgeLock SE05x/A5000 supports the cryptographic requirements and operations defined by TLS v1.2 using both ECC and RSA keys (EdgeLock SE05x only). For ECC keys, both the ECDHE algorithm for key agreement and ECDSA algorithm for digital signatures are supported. AES symmetric keys of up to 256 bits are supported and can be used in ECB, CBC, CTR, GCM and CCM operation modes for data encryption. Finally, the SHA-256 and SHA-384 algorithms are supported as well (EdgeLock SE05x additionally supports SHA-224 and SHA-512). To simplify even more the integration of TLS, the Plug & Trust middleware provides an mbedTLS ALT implementation which allows mbedTLS stack to use the secure element to perform the crypto operations that are part of the TLS handshake between client and server.

The following NXP material can be used as a starting point to meet the requirements listed above:

Table 12. NXP material: secure TLS communication

NXP material	Relevant content
Plug & Trust middleware APIs	• **Perform TLS handshake:** Se05x_API_TLSCalculatePreMasterSecret (), Se05x_API_TLSGenerateRandom (), Se05x_API_TLSPerformPRF()
Plug & Trust middleware demos and examples	• **TLS Client example**: \simw-top\demos\linux\tls_client
Application notes	• AN12400 EdgeLock SE05x for secure connection to OEM cloud

4.2.3 Secure firmware update

The OCPP protocol defines a process for the secure download of firmware updates from the CSMS to the EVSE. The requirements to implement secure firmware update are listed in Table 13.

Table 13. OCPP secure firmware update requirements

Requirement ID	Requirement definition
L01.FR.04	When the Charging Station has successfully downloaded the new firmware, the signature SHALL be validated, by calculating the signature over the entire firmware file using the RSA-PSS or ECDSA algorithm for signing, and the SHA256 algorithm for calculating hash values.
L01.FR.08	It is RECOMMENDED that the firmware is sent encrypted to the Charging Station. This can either be done by using a secure protocol (such as HTTPS, SFTP, or FTPS) to send the firmware, or by encrypting the firmware itself before sending it.
L01.FR.09	Firmware updates SHALL be digitally protected to ensure authenticity and to provide proof of origin.
L01.FR.12	The Charging Station MUST verify the file's digital signature using the Firmware Signing certificate.

Meet L01.FR.04, L01.FR.12: EdgeLock SE05x/A5000 can securely store the public key required to verify the firmware signature. The public key can be protected from deletion and overwriting (or other unintended usage) using secure object policies. For verifying the signature, ECDSA and SHA algorithms are supported (additionally EdgeLock SE05x supports EdDSA and RSA).

Meet L01.FR.08, L01.FR.09: EdgeLock SE05x/A5000 can securely store the ECC private key or the RSA private key (EdgeLock SE05x only) that is required to decrypt a firmware update that has been encrypted using the associated public key. The private key is protected in the SE tamper-resistant hardware and never leaves the boundaries of the SE secure environment. Symmetric encryption / decryption is supported as well using AES (ECB, CBC, CTR, GCM, CCM) and 3DES.

Table 14. NXP material: secure firmware update

NXP material	Relevant content
Plug & Trust middleware APIs	• **Encryption and decryption operations:** sss_asymmetric_encrypt(), sss_asymmetric_decrypt(), sss_cipher_one_go() • **Hashing operations:** sss_se05x_digest_one_go (), Se05x_API_DigestOneShot() • **Sign and verify operations:** sss_se05x_asymmetric_sign_digest (), sss_se05x_asymmetric_verify_digest (), sss_se05x_asymmetric_sign (), sss_se05x_asymmetric_verify (), Se05x_API_RSASign(), Se05x_API_ECDSASign(), Se05x_API_EdDSASign()
Plug & Trust middleware demos and examples	• **Symmetric AES Encryption Example:** \simw-top\sss\ex\symmetric • **Message Digest Example:** \simw-top\sss\ex\md • **ECC Signing Example:** \simw-top\sss\ex\ecc • **RSA Signing Example:** \simw-top\sss\ex\rsa
Application notes	• AN13086 EdgeLock SE05x to enhance the MCU boot sequence security

5 Other recommended enhancements

EdgeLock SE05x/A5000 is a flexible IC that can be used as an all-around solution to implement a wide range of security features and use cases. By integrating EdgeLock SE05x/A5000 in EVSEs it is not only possible to meet the security requirements mandated by smart charging standards and protocols, but also to go beyond that and implement additional, stronger security measures and use cases. For example, an EVSE might benefit from implementing the following features / use cases:

- **Secure boot:** thanks to its anti-tamper features, policy enforcement capabilities and support of modern cryptographic algorithms with high key lengths, EdgeLock SE05x/A5000 provides all the tools required to support the verification of the integrity and authenticity of the firmware during the boot of the EVSE, thus preventing attackers from injecting in the EVSE a corrupted firmware. In fact, EdgeLock SE05x/A5000 can be used as a secure trust anchor for the firmware validation keys and as a secure crypto processor for carrying out related cryptographic operations. Boot security can be improved even more by binding the SE to the MCU so that the MCU can only use the services offered by that particular SE and the SE can only provide its cryptographic services to that particular MCU. More information on secure boot and binding can be found in AN13086 and AN12662.
- **Secure cloud onboarding:** EdgeLock SE05x/A5000 can be used to protect keys and certificates required for the secure authentication and onboarding of the EVSE to a public or private cloud service such as Azure or AWS. To simplify even more the integration, EdgeLock SE05x/A5000 is pre-provisioned with all the certificates and keys required to onboard the EVSE to the most important cloud services. Moreover, the Plug & Trust middleware contains several examples that showcase onboarding and connection to cloud platforms (AWS, Azure, IBM Watson, GCP). More information can be found in AN12401, AN12402, AN12403, AN12404.
- **Updatable applets**: if you integrate **EdgeLock SE051** in EVSEs, you can take advantage of the **SEMS Lite technology** to update applets (e.g. the IoT applet) on-the-field, both online or offline, so as to always get the latest security patches from NXP and the latest updates required to keep up with the ISO 15118 and other specifications as they evolve over time. With EdgeLock SE051, devices can take advantage of the latest features and security improvements as soon as they are available and always enjoy a high protection level for stored credentials. Specific variants of EdgeLock SE051 even allows you to load custom applets so you can implement custom features should they be required by your use case. More information on SEMS Lite can be found in AN12907.

Please refer to EdgeLock SE05x website and EdgeLock A5000 website for the complete list of application notes detailing the supported use cases and how they can be implemented using EdgeLock SE05x/A5000.

6 Legal information

6.1 Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

6.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer. In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages. Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified or documented vulnerabilities. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately. Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

6.3 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Tables

Figures

Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 28 November 2022