Whitepaper
of Charging Interface Initiative e.V.

Interoperability Guide – Public Key Infrastructure (PKI) use cases

Version 2.0

2023-12-08

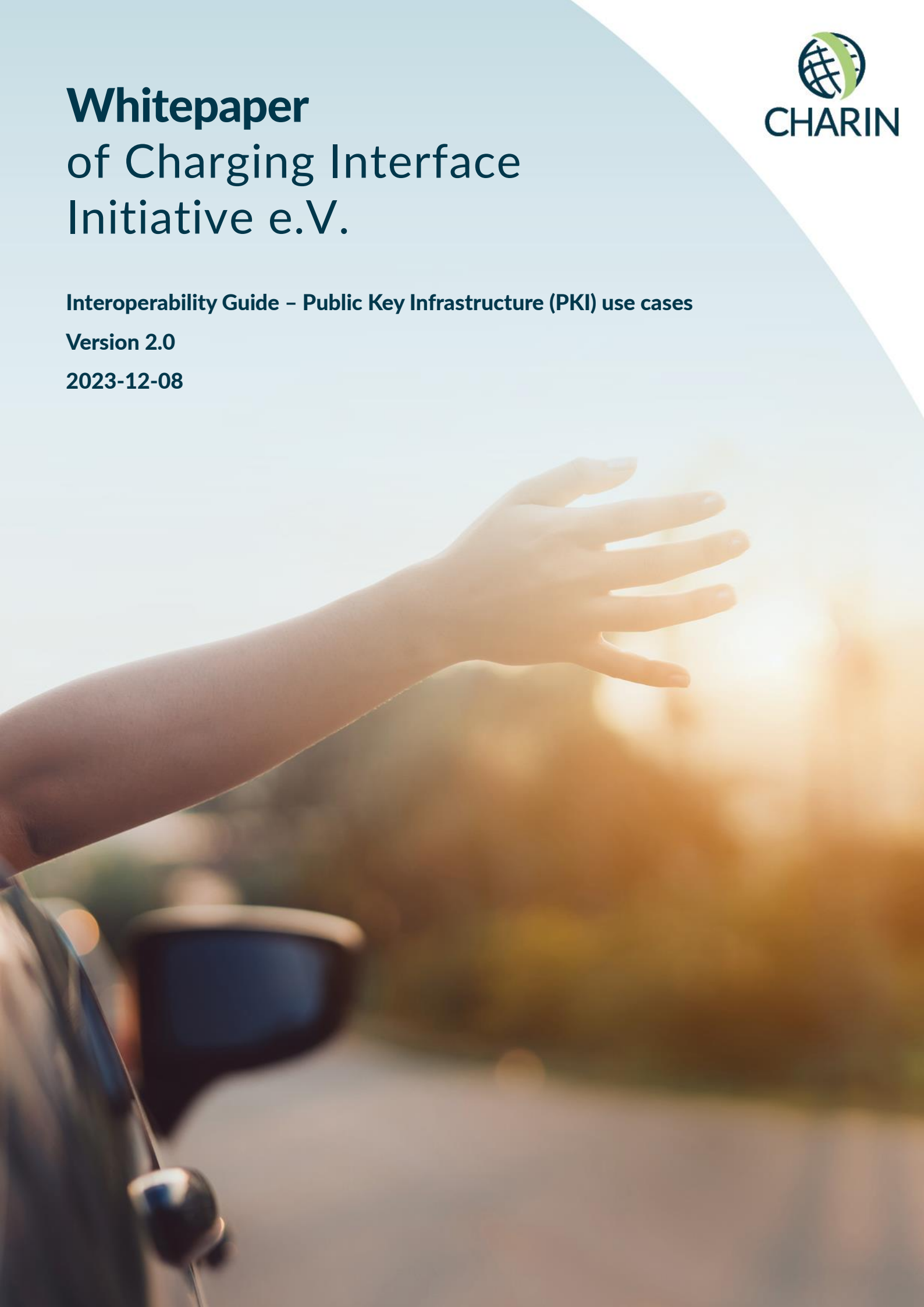


Table of contents

I Purpose of document

The VDE-AR-E 2802-100, the application guide from the German standardization organization DKE titled "Handling of Certificates for Electric Vehicles, Charging Infrastructure and Backend systems within the framework of ISO 15118", defines WHAT each role in the ecosystem must do to allow an EV to obtain its contract certificate bundle through the CSO's charging station or, alternatively, via the OEM backend and install it for future use. Additionally, the VDE-AR-E 2802-100 mandates that an eMSP must generate a contract certificate bundle and deliver it to the Pool of the CPS.

The VDE-AR-E 2802-100 provides the functional basis. Now, CharIN needs to specify the implementation and design of the various IT systems to ensure they become interoperable:

- HOW the individual IT systems of the different roles (eMSP, CPS, CSO and OEM) should technically work together (protocols, etc.).
- HOW the connections between each instance should be technically protected.
- HOW the security of the different OSI layers can be achieved at the same high level.
- HOW the trustworthiness of the OSI layers can be achieved in detail (who receives certificates from which certification authority, certification authorities from which provider, etc.).

The following document currently considers DIN EN ISO15118-2:2016.

The requirements of DIN EN ISO15118-20:2022 may be considered in another version of this document.

Both standards will coexist.

II Reference protocols and standards

The present document refers to the following documents:

- **ISO15118-2**
  Road vehicles – Vehicle-to-Grid Communication Interface
  Part 2: Network and application protocol requirements

- **VDE-AR-E 2802-10**
  Handling of certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO 15118

- **OCPP 2.0.1**
  Open Charge Point Protocol 2.0.1

- **RFC 5280**
  Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

III Symbols and abbreviated terms

Term	Definition	Synonym
CCB	Contract Certificate Bundle	
CCP	Contract Certificates Pool CCP is a data exchange and communication facility, on which the asynchronous (and synchronous) exchanges of Contract Certificates between actors (eMSP, OEM, CSO) is based.	
Certification Authority	A certification authority is an actor in charge of delivering PKI services such as: generation and delivery of certificates, certificate revocation, certificate revocation status publication. It represents the actor and the information system.	CA
Contract Certificate	The contract certificate is an X509 certificate that authenticates the eMSP contract, that will be used to pay the charging sessions. This certificate is issued on behalf the eMSP and must be installed into the EV. It will be used for the charging session authentication step. The Common Name (CN) of this certificate contains the eMAID of the contract	
CP	Certificate Policy	
CSO	Charging Station Operator The CSO is the system actor that manages Charging Points. CSO designates the actor and it's information system. The CSO Back-end system is supposed to be connected to the Charging Stations it manages, and to be able to exchange information and data with them.	CPO (Charging Point Operator)
CPS	Certificate Provisioning Service	
CRL	Certificate Revocation List	
CS	Charging Station	
CSMS	Charging Station Management System, may be local (LCSMS) or remote (CSMS)	CPMS (Charging Point Management System)
CSR	Certificate Signing Request	

Customer	The Customer is the system actor which is the customer of the eMSP who will pay the charging services. EV-Owner, EV-User and MSP-Customer are three separate roles that could be played by 2 or 3 separate actors or by the same actor.	
Directory Service	The Directory Service lists the CCP addresses related to the SCCB / EMAID information, which are used by the CSMS or EV-OEM to install new Contract certificates.	
eMAId	Electric Mobility Account Identifier This is the identifier of the account that the customer has with its eMSP	
EV	Electric Vehicle There is no restriction about the nature of this EV. It could be a car, a bus, a truck, a motorcycle, etc.	
EV-User	The EV-User is the system actor which uses the EV. EV-Owner, EV-User and MSP-Customer are three separate roles that could be played by 2 or 3 separate actors or by the same actor.	
EV-Owner	The EV-Owner is the system actor which has ownership of the EV. EV-Owner, EV-User and MSP-Customer are three separate roles that could be played by 2 or 3 separate actors or by the same actor.	
EVSE	Electric Vehicle Supply Equipment The EVSE is the electric part of a charging station that manages the delivery of energy to the vehicle. The Charging Point is the ability of a Charging Station to charge one vehicle at a time. As there is one EVSE per charging Point and one Charging Point per EVSE, both nouns are synonymous.	Charging Point
EVSEID	Electric Vehicle Supply Equipment IDentifier	
HSM	Hardware Security Module	
IT	Information Technology	
Message broker	The message broker is a central message router for all ecosystem participants described in this document	

MO	Mobility Operator The MO is the system actor that offers services to the customers, and typically the EV Charging services. The customer is supposed to be a customer of a MO and to have an account with the MO. This account is identified by the eMAId.	eMSP (Electric Mobility Service Provider) MSP (Mobility Services Provider), EMP (e-Mobility services Provider)
OCPP	Open Charge Point Protocol	
OCSP	Online Certificate Status Protocol	
OCSP Responder	The OCSP Responder is a service in charge of providing revocation status of certificates. It follows the Online Certificate Status Protocol and creates a signature response by authorization of the upper-level certificate authority that is allowed to manage the OCSP service.	
OCSP Stapling	OCSP Stapling is a means for a server to provide its certificate revocation status, associated ("stapled") to its own certificate, as a means to prevent multiple calls to the OCSP Responder by all clients.	
OEM	OEM stands for "Original Equipment Manufacturer" which is an ambiguous term. In the context of this document, it represents the EV Maker, and thus the actor that designs (engineering) and produces (plant) the EV. This actor is supposed to be able to define the configuration of the vehicle when released from the factory, and to manage the communication link from and to the vehicle.	Car Maker
PCID	Provisioning Certificate Identifier The PCID is an identifier of the EV.	
PCP	Provisioning Certificates Pool PCP is a data exchange and communication facility, on which the asynchronous (and synchronous) exchanges of Provisioning Certificates between actors (eMSP, OEM) are based.	
PKI	Public Key Infrastructure	
PnC/P&C	Plug&Charge	

Private Environment	A Private Environment is defined as a setup of a local area with restricted physical access for EVs equipped with at least one charging station with a private operator certificate chain.	
Provisioning Certificate	The provisioning certificate is an X509 certificate that authenticates the EV. This certificate is issued on behalf of the OEM (of the EV) and must be installed in the EV. The Common Name (CN) of this certificate contains the PCID of the EV.	
RCP	Root Certificates Pool RCP is a data exchange and communication facility, on which the asynchronous (and synchronous) exchanges of RootCA Certificates between actors is based.	
RFID	Radio Frequency IDentifier	
Root CA	A Root Certification Authority is a certification authority that is the root of a PKI hierarchy. It needs to be trusted by all bearers of certificates and by all the parties that will check those certificates. It is represented as a self-signed X509 certificate	
RP	Roaming Platform	
SCCB	Signed Contract Certificate Bundle	
SECC	Supply Equipment Communication Controller The SECC is the ISO15118 communication part of the Charging Station that communicates with the EV. There is only one SECC per Charging Point, but several Charging Point could share the same SECC.	
SECCID	Supply Equipment Communication Controller Identifier This identifier should allow any EV to identify the SECC as a unique entity and check that its authentication certificate matches that SECCID.	CPID (Charge Point Identifier)
SECC Certificate	The SECC certificate is an X509 certificate that authenticates the Charging Station and must be installed into the SECC. It is specific to the Charging station and replaces the formerly used EVSE Leaf	EVSE Leaf Certificate,

	certificate naming. The Common Name (CN) of this certificate contains the SECCID.	Charging Point Certificate
Sub CA	A Sub Certification Authority is a certification authority able to deliver certificates with a trust delegated from a Root CA. There are 2 levels of Sub CA defined for ISO15118. It is represented by a X509 certificate signed by its delivering CA which can be a Root CA or a Sub CA.	
Trust List of Root CA	The trust list of Root CA is the list of Root Certification Authority that are trusted in the whole system. That trust list is a signed list of all the Root Certification Authority certificates or their fingerprints.	CA TL, TL of RCA, Trust Anchors

1. Provision of necessary certificates to operate the Plug & Charge service

This chapter describes all use cases and sub-use cases required for the provision of operation certificates for the PnC service across all stakeholders. Generally, the certificate commissioning process for each stakeholder is carried out in several stages. Some of these stages occur simultaneously (asynchronous data flow) across the various roles and their respective communication paths in the ecosystem.

Various actors participate in the general process: Customer (more precisely the EV-Owner or an authorized person), OEM/OEM-Backend, eMSP, PCP, CPS, CCP, CSO, EV, EVSE, RCP.

Within the process, several asynchronous subprocesses and use cases must occur to provide the necessary certificates for a standardized communication and operation.

- 1.1 Provide certificates for initial setup of each of the PnC service stakeholders
- 1.2 Provide Contract Certificates
- 1.3 Install Contract certificates on EV
- 1.4 Provide certificates for PnC in private environment

It is assumed that all stakeholders will have the required certificates installed in their systems and are ready to operate the standardized and interoperable PnC service.

Within the second level of the processes, several use cases and sub use cases will determine the secure interoperability of the car with the infrastructure. These are described in the subsequent sections.

Below is the structure of the certification authorities and related certificates necessary for the provision of the certificates required to operate the Plug & Charge service:

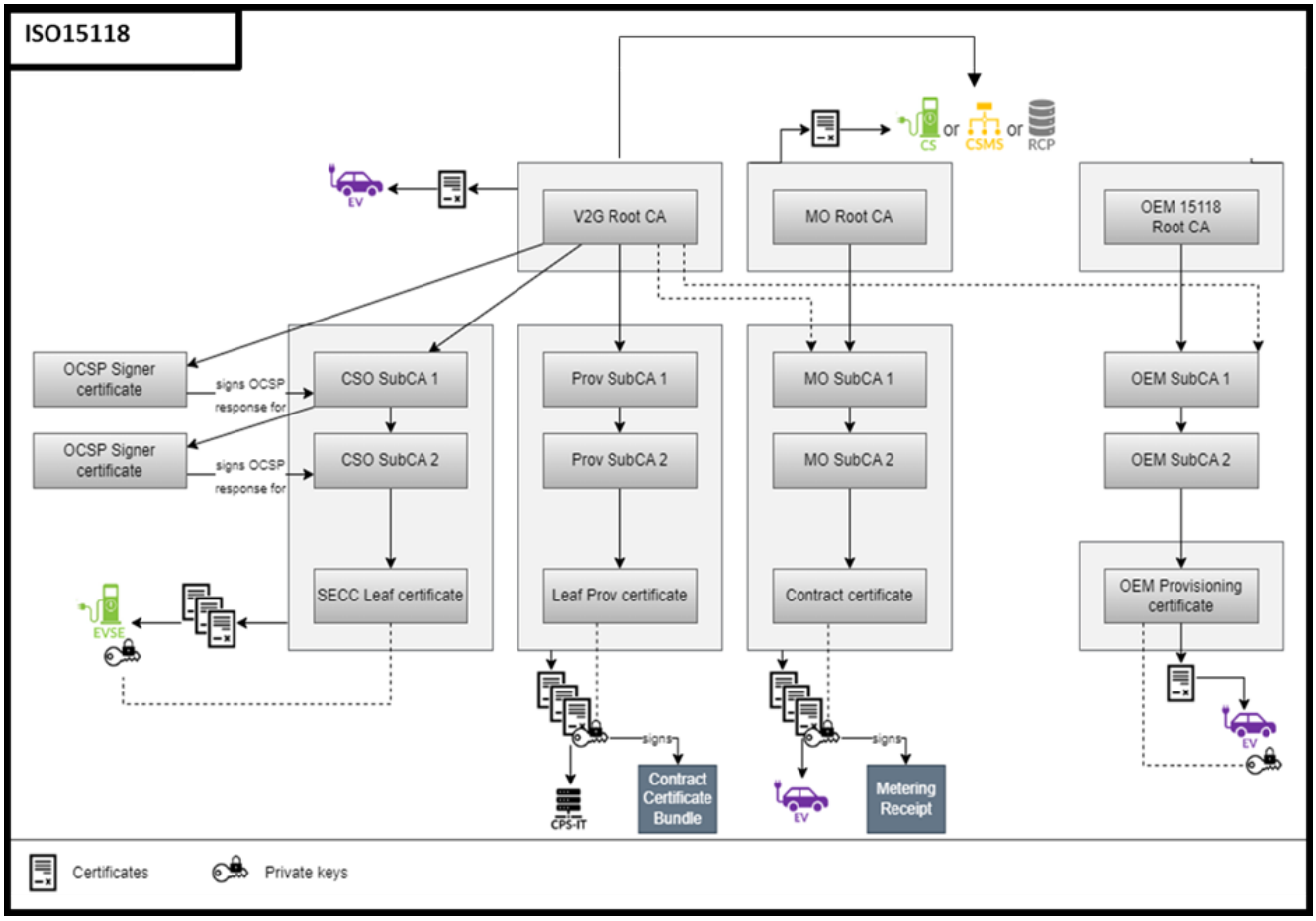


Figure 1: Certificates needed to operate Plug & Charge service.

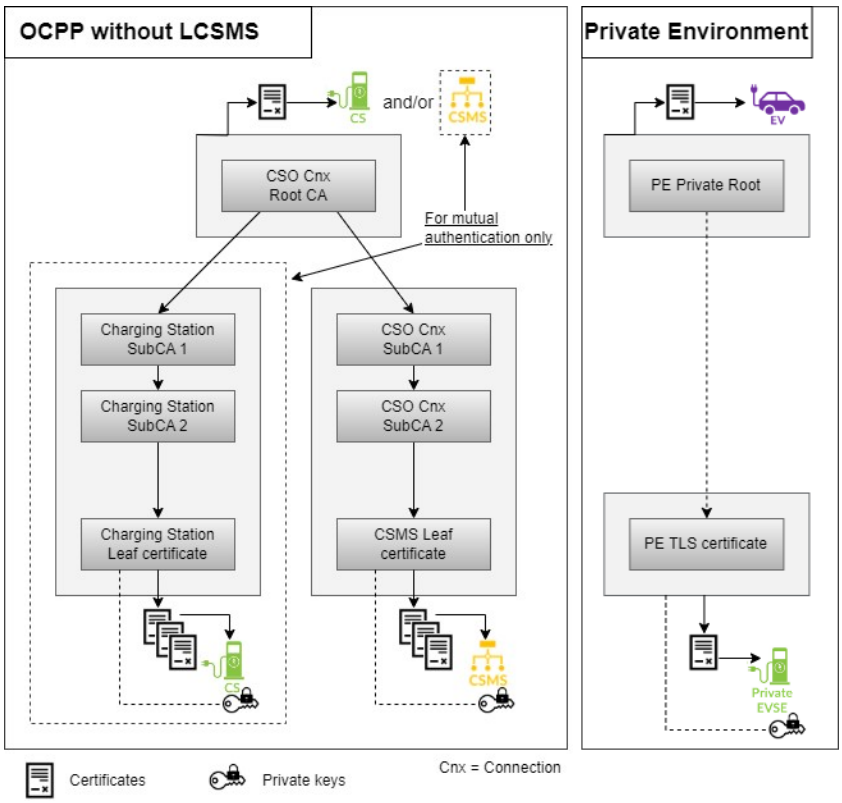


Figure 2: Certificates needed to secure communication between charging station and CSMS, and to operate the service in private environments.

For the initial commissioning or maintenance of embedded systems that transmit data between EV or EVSE and their respective Backends, security needs to be ensured, for example, through certificates within the OEMs.

1.1. Provision of certificates for initial setup of each of the PnC service stakeholders.

This catalogue of use cases will fulfil the objective of providing the Root CA, OEM Provisioning, and SECC leaf certificates to all systems involved in the PnC service operation. This will provide the basic requirements for the ecosystem to function. The following subchapters will outline the responsibilities of the different actors.

The process of commissioning certificates for each stakeholder typically occurs in multiple stages. Some of these stages run in parallel (asynchronous data flow) between the different roles and their respective communication paths in the ecosystem. This is done to obtain the certificate in the provisioning processes for each of the PnC service stakeholders. The actors involved include OEM/OEM-Backend, eMSP, PCP, CSO, EV, EVSE, and RCP.

The following sub chapters and use cases are assumed to take place:

- 1.1.1 Provision of Root CA certificates.
  - 1.1.1.1 Set up a new Root CA and publish the certificates for the PnC service
  - 1.1.1.2 Renewal of Root CA certificates
  - 1.1.1.3 Remove trust in a Root CA certificate
- 1.1.2 Provision of OEM Provisioning certificate
  - 1.1.2.1 Installation of necessary EV certificates
  - 1.1.2.2 Provision of EV data to the PCP
  - 1.1.2.3 Renewal of OEM provisioning certificate at expiry date
  - 1.1.2.4 Renewal of the OEM Provisioning certificate during its validity period
- 1.1.3 Provision of EVSE certificates
  - 1.1.3.1 Installation of relevant certificates in the EVSE to enable the PnC service
  - 1.1.3.2 Update of EVSE certificates to maintain the PnC in service
  - 1.1.3.3 Installation of relevant certificates in the EVSE to enable a secure communication with the CSMS.

1.1.1. Provision of Root CA certificates.

This sub-chapter describes the set up and lifecycle of the Root CA certificates. The use cases address the provisioning of the necessary Root CA certificates required to operate the PnC service.

V2G Root CA certificates have a specific role as trust anchors. As defined in ISO15118, at least one is required to operate the PnC service.

OEMs and eMSPs may have their own Root CAs for OEM Provisioning and Contract certificates respectively. They may also use the V2G Root CAs for their respective certificate provisioning.

The use cases described aim to allow all involved stakeholders to access those Root CA certificates and to verify and trust Leaf certificates from those Root or subordinate CAs.

The involved actors include OEMs, eMSPs, V2G Root CAs operator, RCP.

1.1.1.1. Set up a new Root CA and publish the certificates for the PnC service.

Objective	Set up a new Root CA and publish the certificates for the Plug & Charge service.
Short description	According to ISO15118-2, any role in the PnC ecosystem can operate Root CA. Root CA certificates serve as critical trust anchors. To operate the PnC service, the ecosystem must trust at least one V2G Root CA. OEMs and eMSPs can run their own PKI. One or several Root Certificate Pool (RCP) may be used to supply Root CA certificates in a trustworthy manner, as described in this guide. Root CA certificates can also be exchanged through other secure, ad hoc methods.
Actors involved	eMSP, CPS, CSO, OEM-Backend, V2G Root CA Operator, RCP

Sequence and interface/ Communication channel	• V2G Root CA Operator:
	  ○ Implements a V2G Root CA that complies with the requirements described in the Certificate Policy (CP). These requirements are agreed upon by the PnC ecosystem stakeholders and are established by the CharIN Task Force (link)
	  ○ Generates a V2G root-CA certificate.
	• OEM and eMSP:
	  ○ Optionally, OEMs and/or eMSPs operate (generate / renew) their own Root CA certificates. These certificates are used within their respective PKIs to issue and sign the OEM Provisioning certificates and the Contract certificates.
	• RCP Operator:

	○ Implements a “Trusted Storage Instance for Root CAs" ○ Authenticates and registers parties allowed to operate Root CAs ○ Receives and renews authentic Root CA certificates generated by authorized parties. ○ Saves authentic Root CA certificates centrically for read-only access. ○ Distributes and retrieves authentic Root CA certificates to parties from RCP: RCP may implement notification system to inform parties about changes. ○ Note: For an easy access, the RCP operator may implement a secured API (OPNC) to upload and/or download Root CA certificates.
Precondition/ Requirements	New PKI actor has setup a CA/PKI, but its Root CA is not yet enrolled into the ecosystem. A Certificate Policy and Certificate Practice Statement is available, describing the security level of the new PKI.
Postcondition	At least one V2G Root CA is approved by eMSP(s), CPS(s), CSO(s), OEM(s) and is operative. Every party in the ecosystem has successfully read each other's Root CA Certificate Policy and Certificate Practice Statement. Every Root CA has: • Authenticated and registered to the RCP. • Issued / renewed a valid Root CA certificate for itself and made it available by placing it on the RCP.
Remarks	If an OEM/CSO decides to trust a new PKI actor not listed in the RCP, it’s their responsibility to stablish a process and exchange public key certificates. For a general procedure, we recommend that the new PKI is verified against the CharIN CP, and after the new Root Certificates have been published in RCP.

1.1.1.2. Renewal of Root CA certificates.

Objective	Secure renewal of the trust anchor (Root CA certificate)
Short description	Root CA certificates must be renewed in the following circumstances: • At the end of the validity period • When certain attributes are modified (e.g. DN) This use case describes the regular renewal of a Root CA certificate when it hasn't been compromised. The process for renewing a compromised Root CA certificate is described in UC1.1.1.3, titled "Remove trust from a Root CA certificate."
Actors involved	OEM Backend, CSO, EVSE, eMSP, CPS, RCP
Sequence and interface/ Communication channel	The process of renewing the Root CA certificate largely depends on how the Root CA storage is technically implemented. The renewal operation can be carried out in one of two ways: • Manual update, by an authorized process/person (e.g. USB-stick) • Online update, thought the RCP API (OPNC) If there is a change in the Root CA keys: • Resign or renew the Sub-CAs certificates. Make the new Root CA certificate accessible by publishing it on the RCP. Optionally: Notify the relevant actors in the ecosystem. Retrieve the new Root CA certificates for distribution by every stakeholder (OEM/CSO) to the leaf devices (EV, EVSE, CSMS).
Precondition/ Requirements	Existing valid Root CA certificate available in the RCP
Postcondition	New Root CA certificate published in the RCP
Remarks	Each item signed by a SubCA needs to be renewed. The CA's responsibility is limited to issuing new certificates to a specified destination (e.g., pool, directory). The actors (e.g. CSOs, OEMs) are responsible to download/update those certificates into their respective devices (e.g., EVs, Charging Stations).

	The process of renewing a Root CA certificate is typically lengthy, with both old and new Root CA certificates remaining valid over an extended period. During this process, the old Root CA certificate should not be used to sign new certificates. However, it must stay valid for the sake of validity checks.

1.1.1.3. Remove trust in a Root CA certificate.

Objective	If a Root-CA certificate has been compromised, trusted "third parties" (e.g. CSO, eMSP, OEM, CPS) must "indirectly" notify participants about the compromised Root-CA certificate (and possibly any subordinate CAs). They should also remove Leaf certificates from interim storage. To be more precise • Remove the compromised Root-CA certificate from the RCP. • Remove any other affected certificates and signed content (such as cached OCSP responses or CRLs) issued under the compromised Root-CA.
Short description	Everyone involved typically has an interest or, even better, an obligation to verify the reliability of the used Leaf and CA certificates. If their content verification, such as validity, revocation status, or the trust chain (certificate path) fails, the certificates are deemed untrustworthy. However, if the Root-CA certificate is compromised, an automatic check within a PKI becomes challenging as it is the trust chain's root of this infrastructure. Thus, Root-CA certificates like V2G Root-CAs, OEM Root-Cas, and eMSP Root-CAs need to be withdrawn "indirectly" by a trustworthy "third" party. Removing compromised trust anchors usually requires manual operations by selected and trusted actors. These trusted individuals could include, for example, the operator of a root certificate pool (RCP), a cross-certificate Root-CA or a Root-CA trust list's publisher. In case of a breach, these individuals must be notified by the affected Root-CA operator. They then must remove both the corresponding Root-CA certificate from the RCP and the certificates issued under it from other storages. While this doesn't cover all the obligations of an operator with a compromised Root-CA (which falls within the scope of the Certificate Policy), it outlines a basic procedure like informing affected participants of a trust loss, for instance by removing the compromised Root-CA certificates from the RCP.
Actors involved	Root CA Trust List, Cross-certified Root CA, RCP (Root Certificate Pool), CSOs, eMSPs, OEMs, CPSs
Sequence and interface/ Communication channel	The sequence begins when the Root-CA operator finds out that its Root-CA's private key has been compromised. The operator immediately alerts selected actors who serve as relays for the trust anchor. These may include: • The Root-CA Trust List (if it exists)

	• Other cross-certified Root-CAs (if they exist) • Root Certificate Pools (if they exist) If a Root-CA certificate is compromised, all certificates issued under that Root-CA instantly lose trust. This includes all sub-CA and Leaf certificates issued by this Root-CA, including OCSP responder certificates and CRLs. Essentially, this destroys trust in the entire PKI hierarchy and all OCSP responders become untrustworthy. To maintain PKI operation, the entire hierarchy must be rebuilt. This includes the identity (for example, a new common name) and a new key pair of the Root-CA, and all related PKI instances, such as OCSP responders. The situation becomes particularly devastating when the signatory of the RCP is affected. Then, the RCP or the Certificate Trust List must also be reestablished. From the updated RCP or Certificate Trust List: • The OEM shall remove the Root-CA certificate in the vehicles. • The CSOs shall remove the Root-CA certificate in the charging stations used for verifying contract certificates. • The CPS must identify certificates issued by the compromised Root-CA and refuse to deliver contract certificate bundles. • The eMSP should not generate new contract certificates using the compromised Root-CA. Instead, they should find an alternative Root-CA to deliver them. Unfortunately, if the Root-CA is compromised, charging stations cannot provide reliable proof of certificate revocation status to the EV. There is a possibility that the attacker could also falsify the status in the OSCP. In such scenario, the communication must either terminate the charging station immediately or rely on the OEM to have removed the compromised Root-CA certificate from the vehicle.
Precondition/ Requirements	A Root-CA operator discovers that its Root-CA's private key has been compromised, destroying the security and trust of that Root-CA's entire PKI hierarchy.
Postcondition	The compromised Root-CA certificate has been removed from all directories and caches, e.g., the RCP and the Certificate Trust List. All certificates and signed data issued and derived under the compromised Root-CA have been removed from all participants.

Remarks	Immediately after receiving the first notification of the Root-CA's private key compromise, the operator of this PKI must promptly evaluate the situation and initiate actions to prevent damage per the emergency plan. The Root-CA must provide a timeline to restore normal PKI operation by setting up a new PKI hierarchy.

1.1.2. Provision of OEM Provisioning certificate.

The aim of this sub chapter is to define how the OEM initially provides provisioning and vehicle identities, which are linked to asymmetric keys generated in the EV. It also explains how the OEM renews this key material throughout the EV's life cycle.

Actors involved are:

- OEM IT Backend,
- EV,
- RCP (Root Certificate Pool),
- PCP (Provisioning Certificate Pool).

Prerequisites:

- The OEM maintains a registration authority within its IT organization (OEM RA) that registers the identities required for the provision of the contract certificate and the access to the charging infrastructure.
- The OEM has a certification authority within its IT organization (OEM CA) that associates these identities with the corresponding public keys for the EV and issues the Leaf certificates.
- The OEM IT backend has securely provided its OEM Root CA certificate, OEM Provisioning certificates, and the OEM Sub CA certificates to the eMSPs and the relevant certificates pool(s).
- The OEM has the capability to automatically install these leaf certificates in the EV hardware both during production and in the workshop, serving as a root-of-trust.
- The OEM can automatically renew these Leaf certificates over the electric vehicle's life cycle through its telematics connection (i.e. over-the-air) and/or in the workshop.
- The OEM has registered the necessary identities for the provision of the contract certificate and the EV's charging infrastructure access within its certification authority (OEM CA)
- The OEM has linked these identities to the corresponding public keys for the EV in its OEM CA and issued the Leaf certificates.
- The OEM has securely and automatically stored these Leaf certificates in the EV hardware as a root-of-trust, initially during production and in the workshop.
- The OEM can automatically renew these Leaf certificates before expiry over the vehicle's life cycle through its telematics connection (i.e. over-the-air) and/or in the workshop.

1.1.2.1. Installation of necessary EV certificates.

Objective	Preparation of an EV to communicate with the charging infrastructure in accordance with ISO15118-2, either during or after EV production process.
Short description	Install all necessary certificates in the EV, either during or after its manufacturing: • OEM ISO15118 Root certificate • V2G Root certificate(s) • EV Manufacturer Root certificate(s) • OEM Provisioning certificate and corresponding private key Considering the following two steps in this process: • The OEM IT gathers the credentials. • The OEM IT installs the credentials in the EV.
Actors involved	OEM IT, EV, RCP
Sequence and interface/ Communication channel	The OEM IT backend should ensure the following: • The OEM IT backend and the RCP have authenticated each other and established a connection. • The transfer of its OEM ISO 15118 Root CA certificate and, if applicable, OEM sub-CA certificates to the RCP in a secured container (trust store container as defined in VDE-AR-E 2802-100, Appendix C). The RCP should validate and securely store these certificates. • The retrieval of the required V2G Root CA certificates from the RCP and, if applicable, PE (private environment) Root CA certificates (as outlined in VDE-AR-E 2802-100, 11.2.2) in a secure container (also defined in VDE-AR-E 2802-100, Appendix C). These certificates should be validated and securely stored. • The OEM IT backend transfers the OEM ISO 15118 Root, V2G Root and EV Manufacturer Root certificates to the EV for installation. • The EV generates the necessary keys in its secure storage (with the ECU handling the private key). • The EV establishes a mutually authenticated and secure connection with the OEM IT backend.

	• The EV requests its individual OEM Provisioning certificate, including the OEM SubCA certificates, from the OEM IT backend, validates the OEM Provisioning certificate, and securely stores it with its private key.
Precondition/ Requirements	The OEM IT can securely and mutually authenticate communication with the RCP, provided that both sides possess the necessary certificates. The OEM IT operates a certificate issuer instance. Similarly, the EV can securely and mutually authenticate communication with the OEM IT backend, which also requires necessary certificates from both sides. This can be accomplished via trust-lists or cross-certification. The EV has already been assigned a PCID. It uses secure key storage which could be a Trusted Execution Environment, HSM, or Trusted Platform Module 2.0. For a secure implementation of the trust store container for Root-CA certificates, refer to VDE-AR-E 2802-100, Appendix C.
Postcondition	The EV possesses the following: • It is registered and authenticated with the OEM IT backend, ensuring mutual authentication and secure communication. • It holds valid OEM ISO 15118 Root and EV Manufacturer Root certificates from the OEM, which are securely stored. • It has securely stored all relevant V2G Root CA certificates (at least one). • If required, Root CA certificates from private operators (refer to VDE AR Appendix C) are also securely stored. • The EV individual provisioning certificate issued by the manufacturer and the associated private key are securely stored.
Remarks	Note: The OEM IT backend should also make its root-CA accessible for other participants (process 1.1.2.2.).

1.1.2.2. Provision of EV data to the PCP

Objective	OEM Provisioning certificate has been generated and is available in PCP.
Short description	EV certificate (OEM Provisioning certificate) is provisioned to the PCP
Actors involved	OEM IT Backend, EV, PCP
Sequence and interface/ Communication channel	The OEM IT Back-end and the PCP establish a secure communication channel. The OEM IT Back-end then transmits the OEM provisioning certificate to the PCP. This certificate includes data about the V2G Root CA supported by the EV, ISO 15118 supported version: XML schema namespace (e.g. "urn:iso:15118:2:2013:MsgDef"), as well as the OEM Provisioning certificate chain. This data informs the PCP about the supported ISO-version and EV-HSM support. The PCP stores the certificate for future use and makes it available to relevant parties (e.g. eMSP). If applicable, the PCP may also provide information about the availability of a new EV provisioning certificate package.
Precondition/ Requirements	EV is in production phase or already built (part replacement). 1.1.2.1 Installation of necessary EV certificates: OEM Root certificate is published in the RCP.
Postcondition	The OEM Provisioning certificate is created, supplied to the PCP, and made accessible to eMSPs.
Suggested technical solution / req. to ensure interoperability	Certificate must be ISO 15118-2 standard compliant. OEM – PCP communication protocol must be aligned

1.1.2.3. Renewal of OEM provisioning certificate at expiry date

Objective	The renewed OEM Provisioning certificate will be generated and made available in the EV and to the PCP.
Short description	Before the expiration date, the OEM Provisioning certificate will be renewed and provisioned into the EV and to the PCP.
Actors involved	OEM IT Back-end, EV, PCP
Sequence and interface/ Communication channel	The private/public key pair may be changed by the OEM (or EV). The OEM IT Backend creates a renewed OEM provisioning certificate for EV. OEM IT Backend and PCP establish a secure communication channel. The OEM IT Backend sends the updated OEM Provisioning certificate and related EV information to the PCP. The PCP then stores the renewed certificate, removes the old one, and makes it accessible to relevant parties (e.g., eMSP).
Precondition/ Requirements	The OEM IT identifies the need to update an EV's OEM Provisioning certificate by monitoring its expiration date: Current OEM Provisioning certificate is about to become invalid, expired or revoked, and a succeeding OEM Provisioning certificate is not created yet.
Postcondition	Renewed OEM Provisioning certificate is created, provisioned to the PCP and made available to the eMSPs.

1.1.2.4. Renewal of the OEM Provisioning certificate during its validity period.

Objective	A renewed OEM Provisioning certificate is generated and made available in the EV and to the PCP.
Short description	This use case addresses the update of non-revoked OEM Provisioning certificates within their validity period. Two situations must be considered: PCID not changed: • Pros: The identity of the EV remains unchanged, resulting in less impact on the end user and the eMSP (due to PCID/EMAID correspondence). • Cons: The initialization process may become complex involving information from the old OEM Provisioning certificate, deletion of cached certificates (eMSP /CPS), and managing any Bundles waiting for installation on the EV. If EMAID/Contract certificates are removed from the EV, provisioning and installation with the eMSP must start over. New PCID: • Pros: There is no risk of reusing the old OEM Provisioning certificate. The initialization process is simpler, and no particular procedure is needed to manage the old OEM Provisioning certificate (cache, bundles, etc). • Cons: The contract certificate installation process becomes more complex. Everything must be redone based on the new PCID, posing a risk of significant impact on the EV-User.
Actors involved	OEM (EV), PCP, eMSP
Sequence and interface/ Communication channel	The OEM detects the need to update the OEM Provisioning certificate of an EV. The previous OEM Provisioning certificate is revoked. This step can be postponed if the renewal is not security related. Private/public key pair may be changed by the OEM or the EV. Execute UC 1.1.2.1: Install EV necessary certificates. Execute UC1.1.2.2: Provide EV data to PCP. If PCID is not changed: • The OEM associates the the new OEM Provisioning certificate with the PCID;

	• The OEM informs eMSP /CPS to remove the cached OEM Provisioning certificate and prepare for the installation of Contract Certificate Bundles for the EV; • If the EMAID/Contract certificate is removed from the EV, the OEM should request eMSP(s)/CPS to re-provision the contract certificate bundle for contract certificates installation. In case of a new PCID: • The OEM obtains or creates the new PCID for the EV; • The OEM communicates the new PCID to the EV-User; • The OEM may add the old PCID to the vehicle data stored in the PCP; • Following the OEM procedure, either the OEM or the EV-User informs the eMSP to create a new Contract Certificate Bundle for the EV.
Precondition/ Requirements	Updated OEM Provisioning certificate is not created.
Postcondition	The renewed OEM Provisioning certificate is created, installed in the EV, and made available to eMSPs through provisioning in the PCP. The EV is now prepared for the installation of Contract certificates as outlined in UC1.3 Install Contract certificate on EV

1.1.3. Provision of EVSE certificates

This sub chapter describes the responsibilities of the CSO in preparing EVSEs to support the PnC service by providing the required certificates: SECC certificate chains and Root CA certificates.

This only includes the initial commissioning and the necessary updates over time by the CSO.

The actors involved are:

- CSO
- EVSE
- RCP
- OCSP Responder

Prerequisites:

The CSO must be registered to or operate a V2G Sub CA to sign SECC leaf certificates and have the means to install certificates at the EVSE or be able to contract someone to do so.

The EVSE must be provided with the necessary certificates to operate the PnC service:

- Mandatory
  - Authentication certificates for secure communication with the EVs, including the certificate chain up to but excluding Root CA certificate,
  - Authentication certificates for secure communication with the CSMS when appropriate,
  - Trust anchors: eMSP Root CAs should be installed in EVSE or CSMS.
- Recommended
  - V2G Root CA certificate(s) should be installed to allow validity check for SECC certificate chain renewal.

1.1.3.1. Installation of relevant certificates in the EVSE to enable the PnC service

Objective	Make the EVSE ready to operate the PnC service
Short description	To prepare an EVSE for the PnC service, the following steps are required: • Manage certificates for both ISO 15118 and OCPP communications. • Activate both ISO 15118 and OCPP communications. In order for a CSO to prepare a Charging Station for PnC service, the manufacturer needs to provide instructions for installing the relevant PnC certificates: • The SECC leaf certificate and associated trust chain, which secure the communication between the Electric Vehicle and the ISO 15118-2 communication controller (SECC); • eMSP Root certificates which authenticate the contract certificates if the Charging Station conducts contract certificate validation; Recommendations: • Install at least one V2G Root CA certificate, the trust anchor connected to the SECC leaf certificate Note: For secure system initialization or charging station maintenance, the Charging Station manufacturer should install its own CS Manufacturer Root certificate during production. This process is not covered in this document.
Actors involved	Charging station (EVSE), CSO, Charging Station Management System (CSMS), V2G Root CA/SubCA, RCP, OCSP Responder
Sequence and interface/ Communication channel	• The CSMS establishes communication with the EVSE. • The CSMS obtains the relevant Root Certificates from the RCP, including the V2G Root and eMSP Root certificate. • Depending on the specific requirements of the EVSE, the CSMS installs the EVSE Trust Anchors: the V2G Root, eMSP Root and CSO Root certificates. • The CSMS requests the EVSE to start Leaf Certificate creation. • The EVSE generates a new pair of private and public keys. • The EVSE generates a CSR (Certificate Signing Request) to be signed by a SubCA of the V2G Root CA, which includes the SECCID.

	• The EVSE sends the CSR to the CSMS. • The CSMS forwards the CSR to the SubCA. • The SubCA generates the SECC leaf certificate, signs it and returns it to the CSMS. • The CSMS sends the signed certificate, along with its related certificate chain, to the EVSE. • The EVSE verifies the signed certificate. • The EVSE requests the CSMS to provide the OCSP responses for the entire trust chain of the SECC leaf certificate, excluding the V2G Root certificate. • The CSMS requests the OCSP Responder to provide an OCSP response for the SECC Leaf certificate and returns it to the EVSE upon reception. Note: The EVSE should regularly renew the OCSP response before expiry date (for example, on a weekly basis). • The CSMS requests the EVSE to activate the PnC service.
Precondition/ Requirements	The Charging Station (including the EVSE) supports the PnC service, meaning that ISO 15118-2 and OCPP2.0.1 communication protocols have been implemented, but the function is not yet activated. None of the PnC related certificates are installed in the EVSE. This includes the EVSE Leaf, CSO SubCA, V2G Root, and eMSP Root certificates. The certificate installed is the EVSE Manufacturer Root certificate. The EVSE and the CSMS have established a trusted and secure communication channel.
Postcondition	The PnC service is activated in the EVSE: Both ISO 15118 and OCPP communications are operational. The required certificates (for instance the eMSP Root, the V2G Root CA certificates, and the CSO Root certificate) are deployed in the charging station.

Suggested technical solution / req. to ensure interoperability	For the optional installation of the CSO Root CA:
	  • It's better for the EVSE manufacturer to handle it.
	  • Utilizing the Registration service (provider by either the CSO or EVSE Manufacturer) might improve operations.
	• Employing the V2G Root CA could simplify this provisioning

1.1.3.2. Update of EVSE certificates to maintain the PnC in service.

Objective	PnC relevant EVSE certificates are up to date.
Short description	The Charging Station or the managing CSMS initiates the certificate update request when it detects that its SECC leaf certificate, the V2G Root certificate, or the eMSP Certificates (if any) are nearing their expiry date. Recommendations: • Update Leaf certificates one week prior to their expiry date. • Update Root certificates one month prior to their expiry date. Important: The certificate's revocation triggers the update process.
Actors involved	EVSE, CSO, CSMS, Sub-CA/Root CA, RCP
Sequence and interface/ Communication channel	If the certificate to be renewed is the SECC leaf certificate: • Optional: The EVSE generates a new pair of private/public keys. • The EVSE generates a CSR (Certificate Signing Request) for signature by a SubCA of a V2G Root CA; • The EVSE sends the CSR to the CSMS; • The CSMS forwards the CSR to the SubCA; • The SubCA signs the certificate and returns it to CSMS; • The CSMS sends the signed certificate (including the certificate chain) to the EVSE; • The EVSE verifies the signed certificate; • The EVSE requests the OCSP response of the Leaf certificate from the CSMS; • The CSMS requests the OCSP Responder to provide an OCSP response for the SECC leaf certificate and returns it to the EVSE upon receipt; • Note: The EVSE should regularly renew the OCSP response before expiry date. If the certificate to be renewed is a Trust Anchor (Root CA certificate): • The EVSE requests the CSMS to renew a Root certificate; • The CSMS obtains the requested Root certificate(s) from the RCP; • The CSMS forwards the requested Root certificate to the EVSE.
Precondition/ Requirements	The EVSE is operating the PnC service.

	The EVSE and the CSMS have established a trusted and secured communication channel. The EVSE detected a need for a certificate update.
Postcondition	The EVSE certificates are up to date.

1.1.3.3. Installation of relevant certificates in the EVSE to enable a secure communication with the CSMS

Objective	Prepare the Charging Station to facilitate secure communication with the CSMS. This will enable operation of the PnC service while adhering to cybersecurity requirements.
Short description	This use case describes the security requirements the Charging Station and the CSMS shall implement before operating the PnC service.
Actors involved	CS, CSO, CSMS, CSO Root-CA/Sub-CA, (Charging Station Manufacturer)
Sequence and interface/ Communication channel	The CSO CA (or SubCA) issues an X509 certificate to the CSMS in accordance with OCPP 2.0.1 requirements. At initialization: • The CSMS authenticates itself using the CSMS Leaf certificate as the server-side certificate; • Optional: For client (mutual) authentication, the EVSE authenticates itself by using the Charging Station Leaf certificate as the client-side certificate. Verification: • The EVSE verifies the certification path of the CSMS Leaf certificate; • For client (mutual) authentication, the CSMS verifies the certification path of the Charging Station Leaf certificate. To allow the EVSE to authenticate to the CSMS, provide a username and password: • The username should be the Charging Station Identity • The password should be random • Ideally, the EVSE Manufacturer should prepare the username and password. • A registration service could be used to update the connection profile of the Charging Station prior to the initial connection to CSMS.
Precondition/ Requirements	Both the EVSE and the CSMS must support at least version TLS 1.2. However, TLS1.3 or higher versions are recommended.

	The CSMS acts as the TLS server, while the EVSE functions as the TLS client. The CSMS should support TLS with basic authentication (server authentication) or a client-side certificate (server and client authentication). The EVSE must be able to support a client-side certificate (server and client authentication). This use case adheres to the OCPP 2.0.1 specifications. For state-of-the-art security, the implementation of mutual TLS using client-side certificate (server and client authentication) is recommended. If the EVSE needs to be configured with a specific CSO Root CA certificate, it must be installed on the EVSE beforehand.
Postcondition	The CSMS and the EVSE are prepared to initiate a TLS communication

1.2. Provision of Contract Certificates

The common goal of the use cases discussed in this section is to outline the necessary steps for managing certificates, from the initial eMSP customer request to the eventual publication of the Signed Contract Certificate Bundle in a Contract Certificate Pool. This pool can be accessed by OEMs and CSOs for car installation.

The described use cases outline each step, starting from the subscription to an eMSP up to the delivery of the Contract Certificate into the Contract Certificate Pool (CCP) or equivalent.

This section introduces the concept of a default Signed Contract Certificate Bundle, which is prepared in the CCP for download and installation through the charging station process (as per UC 2.3.1). This default SCCB is the first one added to the pool, ensuring that there is always a contract certificate available for installation onto the EV during its first charge.

However, there is a drawback to this approach. The installation and activation of a contract certificate for an EV-Driver sets the price of the charge (based on the mobility contract) and therefore cannot be changed without the payer consent and knowledge.

Several actors are involved in the subprocess:

- EV-User,
- eMSP,
- OEM,
- CPS,
- CCP

The following asynchronous processes facilitate certificate provisioning:

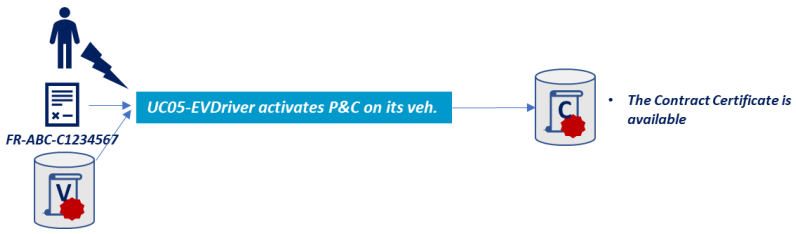
- 1.2.1 Subscription to the PnC service: Contract certificate creation
- 1.2.2 Preparation of the Contract Certificate Bundle (CCB)
- 1.2.3 Signature of the Contract Certificate Bundle
- 1.2.4 Storage of the Signed Contract Certificate Bundle in the CCP
- 1.2.5 Renewal of the Contract certificate from the eMSP
- 1.2.6 CCP cleanup

These use cases operate under the precondition that the certificates for other actors are already set up and ready, as outlined in paragraph 1.1 use cases. In particular, the EV referred to in these use cases must have been initialized with a valid Provisioning Certificate, and PKI Services for the Root CA must be set up for the CPS.

Another requirement is for the EV-User to have a subscribed mobility contract with the eMSP. This subscription is not described in this document as it does not involve the use of certificates.

Lastly, the EV-User must have access to the EV's PCID, based on information chosen by the OEM. Paragraph 1.2.1 proposes a list of alternatives for information purposes only, and this list is not exhaustive.

1.2.1. Subscription to the PnC service: Contract certificate creation

Objective	The eMSP obtains the OEM Provisioning Certificate linked to the target EV, creates a new EMAID if needed, and generates a Contract Certificate in line with the ISO 15118-2 specification.
Short description	The EV-User obtains the PCID of the EV through any means provided by the EV-OEM. Some recommended options are listed below. The EV-User subscribes to an eMSP that supports PnC features and activates PnC. The EV-User must provide the vehicle's PCID to the eMSP. For additional control only, see §5. When activating PnC for a specific EV, the eMSP customer should have the option to determine if they need advanced authorization, which specifies which EV-driver can use this contract certificate for payment. They should be reminded that authorization will not be required at the time of charging but may only be necessary when configuring the contract certificate. Once all prerequisite checks are complete, the eMSP: • Generates an EMAID for the customer (if not yet done), • Generates the Contract Certificate 
\Actors involved	EV-User, eMSP, PCP, (OEM), (CPS)
Sequence and interface/ Communication channel	The EV-User begins the process by requesting the PnC feature activation from their eMSP. Next, the EV-User obtains their PCID. The options include (but are not limited to): • Physical methods for exchanging digital information such as smartphone apps, vehicle Human Machine interface (HMI), web interfaces, etc.

	• Digital methods for extracting information such as Object Character Recognition (OCR), QR Codes, Authentication Frameworks (like OAuth2.0 or similar), etc. • Non-digital backup solutions provided by the OEM (not required in case of a purely online relationship) Considering the strengths and weaknesses below, it is recommended that the customer obtains the PCID as a human-readable string and computer-readable QR code from an HMI (like and EV or App) AND/OR an authentication framework with automated PCID data transmission to the eMSP. The OEM then defines security measures to protect the EV from PCID misuse, such as unintentional contract certificate installation. For instance, any newly installed contract certificate at the EV should not be activated before the EV-User approves it. 1. The EV-User transmits the vehicle's PCID to the eMSP. • The OEM provides the PCID to the eMSP customer in a user-friendly way. • The eMSP customer receives the PCID. 2. The eMSP accesses the Provisioning Vehicle Certificate using the PCID. • This can be requested from the OEM (since the PCID contains the OEM's ID). • Or it can be accessed via the corresponding PCP. 3. The eMSP creates and signs the Contract Certificate. • The contract certificate's validity period should not exceed the remaining validity period of this EV's provisioning certificate.
Precondition/ Requirements	The eMSP customer becomes the (delegated) owner of an electric vehicle and wants to stablish an eMSP contract for that vehicle with PnC and roaming according to their chosen terms. This eMSP contract could be new or pre-existing. The EV-User has access the PCID of the corresponding EV. Based on a valid PCID, the eMSP can identify the OEM or the PCP willing to share Vehicle Data (such as EV Provisioning certificate, V2G Root CA certificate ids), and the eMSP may utilize PCP services for this purpose. The EV-User has an active subscription to an eMSP service.

	The vehicle is PnC ISO 15118-ready. The EV-User has all the necessary permissions to activate the PnC service on the associated EV.
Postcondition	The contract certificate is available to be incorporated in a Contract Certificate Bundle.

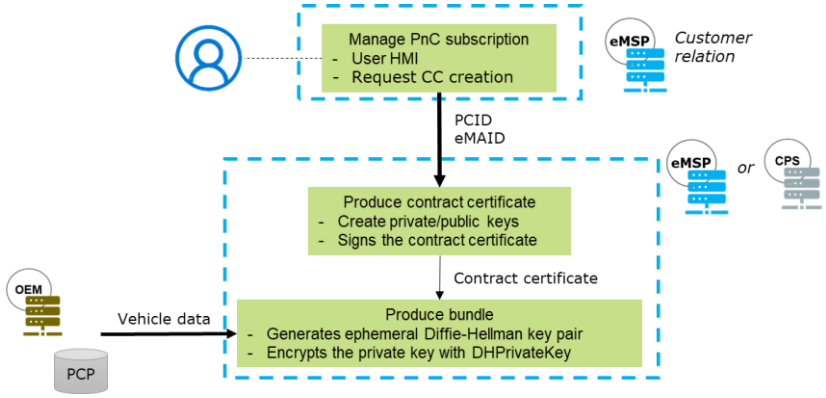
Note: The following section describes the options that an OEM could provide to customers for PCID retrieval:

1) **The OEM includes the PCID in the vehicle information sheet.**
   - Pros
     - The PCID is easily made available to the customer.
   - Cons
     - The PCID could change, becoming outdated. It could be difficult to obtain the latest PCID from the OEM. The delivery method is not secure and requires the customer to manually type the PCID into the e-Mobility Service Provider's system.
2) **The PCID is displayed on the vehicle's user interface.**
   - Pros
     - The PCID could be secured with a PIN code or other methods.
     - The PCID could be provided in a way familiar to the customer, such as scanning a QR code or entering credentials through linked account's API. This method follows the telecommunications industry's standards, making the chosen solution future-proof.
   - Cons
     - The customer must either be physically present in the car or use the EV OEM application to obtain their PCID.
3) **The PCID is available on the OEM portal and/or on the OEM App.**
   - Pros
     - The customer can retrieve his PCID from outside the vehicle.
   - Cons
     - The customer must have an OEM account.
     - This process is not standardized, potentially leading to various solutions by the OEMs. This could cause customer friction due to unfamiliarity with the system (e.g., a dedicated call-centre might be necessary).
4) **Implementing an authentication framework allows the OEM to supply the PCID directly to the eMSP.**
   - Pros
     - The process can be conducted outside of the vehicle.

- The provisioning process can be fully automated, preventing the user from mistyping the PCID.

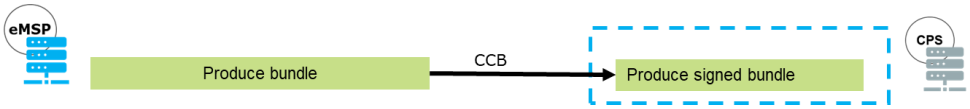
- Cons
  - The customer must have an OEM account.
  - For some use cases, third party users (non-owners) might need special access to the OEM account with restricted access rights (e.g.: for professional purposes such as vehicle fleet management).

1.2.2. Preparation of the Contract Certificate Bundle (CCB)

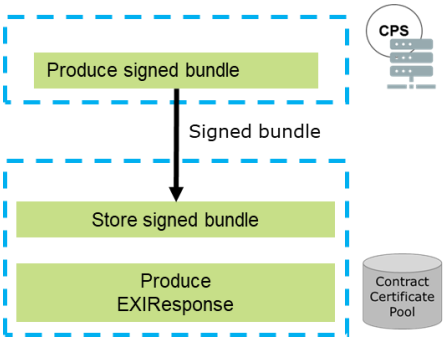
Objective	Generate a "ready-to-sign" CCB, including the contract certificate, the encrypted private key, and the vehicle's meta-data.
Short description	The previous use case 1.2.1 concerns the preparation of the EMAID and the Contract certificate. This use case details the extra steps required to create the CCB, a self-contained, signed, and secure standard package containing the essential elements for contract certificate installation. 
Actors involved	eMSP, CPS
Sequence and interface/ Communication channel	The eMSP or delegate retrieves the EV metadata using the PCID contained in the Contract Certificate. The eMSP or delegate generates an ephemeral Diffie-Hellman key pair as specified by ISO 15118. The eMSP or delegate encrypts the private key related to the Contract certificate with the Diffie-Hellman private key (generated previously) as specified by ISO 15118. The eMSP or delegate gathers every required information into a single CCB object, including: • the Contract certificate and related trust chain, • the encrypted private key, • the EV metadata, such as PCID, list of supported V2G RCA, and supported versions of ISO 15118. The eMSP or delegate then provides the CCB to a CPS for signature (ref. use case 1.2.3).

	[Additional control only (see §5)] Additionally, the eMSP should include information about whether further additional authorization is needed. This information could be added to the contract certificate itself, the CCB, or as a metadata of the CCB stored in the pool.
Precondition/ Requirements	Subscription to the PnC service: Contract certificate With a valid PCID, the CPS can identify the OEM or the PCP that is ready to share the Vehicle Data (EV Provisioning certificate, V2G Root ids…). The CPS may use PCP services for this purpose.
Postcondition	The CCB is ready to be signed by a CPS.

1.2.3. Signature of the Contract Certificate Bundle

Objective	The Signed Contract Certificate Bundle is made available to be pushed to the contract certificate pool, or directly to the OEM or CSO.
Short description	Under the use case 1.2.2, the CPS signs the Contract Certificate Bundle (CCB). This results in a Signed Contract Certificate Bundle (SCCB) that is ready to be provisioned at CCP (or OEM, CSO). If the installed V2G Root CAs at the EV side are known, compatibility with the EV can be ensured by having the signer possess a signing certificate from one of these supported V2G Root CAs. In case the installed V2G Root CA are unknown, it is feasible to prepare multiple SCCBs to cover various V2G Root Cas. This strategy maximizes the chances of compatibility with the installed V2G Root Cas in the EV. 
Actors involved	(eMSP), CPS
Sequence and interface/ Communication channel	Following operations are performed by the CPS: • Request contract certificate bundle signatures to all registered signers available. • Sign the contract certificate bundle. After these steps, all the SCCBs prepared for communication to the CCP, or directly to the OEM or CPO.
Precondition/ Requirements	Preparation of the Contract Certificate Bundle (CCB). Each CCB signer, whether a CPS or eMSP, is a subCA1 or subCA2 of a V2G Root CA. This is likely to be supported by the associated EV. Then contract certificate bundle is then provisioned to the CPS.
Postcondition	The Signed Contract Certificate Bundle is ready for provisioning either to the CCP or directly to the OEM/CPO).

1.2.4. Storage of the Signed Contract Certificate Bundle in the CCP

Objective	Make the Signed Contract Certificate Bundle (SCCB) available at a CCP for installation by the OEM or the CSO.
Short description	Once the CPS signs the CCB, the SCCB is made available for installation at the CCP. 
Actors involved	CPS, (eMSP), CCP.
Sequence and interface/ Communication channel	The actor that holds the SCCB (either eMSP or CPS) publishes the SCCB at a CCP: • The eMSP or CPS establishes secure communication with the CCP, • The eMSP or CPS sends the SCCB to the CCP, • The CCP verifies the SCCB signature and confirms reception, • If the CCP supports notifications, it notifies subscribers about the newly available SCCB. • The CPS needs to add the CPS V2G root identifier, which was used for signing, to the SCCB and ISO 15118 version. • The initial SCCB published for a specific PCID should always be marked as default. [Additional control only (see §5)] If the driver needs additional authorization to use that contract certificate, this information should be stored. It could be in the contract certificate itself, in the CCB, or as a metadata of the CCB in the pool. Note: The CCP must convert the SCCB into an EXI format (as specified in ISO 15118). If the CSO installs it over ISO 15118, the translation to EXI format occurs upon request reception from the CSO, as it relies on the ISO 15118 communication session information.

Precondition/ Requirements	Signature of the Contract Certificate Bundle
	
	The eMSP or CPS has already established contractual relationship with at least one CCP and is capable of setting up secure communication with the CCP.
	
	Recommendations:
	• If there are multiple CCPs available, the CPS should ensure that the chosen CCP allows the distribution of the SCCB to the targeted EV.
	• To enhance interoperability:
	  ○ CCP operators implement the same APIs (OPNC).
	  ○ CCP operators should organize themselves to ensure interoperability and cooperation, guaranteeing SCCB distribution.

Postcondition	SCCB available for installation by OEM or CSO at CCP.

1.2.5. Renewal of the Contract certificate from the eMSP

Objective	Ensure the contract certificate remains updated to prevent any interruptions in payment authorizations from the EV due to certificate expiration.
Short description	The use of the PnC service depends on a valid contract certificate stored in the car. The charge point verifies this certificate before starting the charge. If the contract certificate has expired, the charge point will not allow the car to be charged. This use case describes how the eMSP renews the contract certificate. The eMSP should only automatically renew the contract certificate if the customer has chosen to allow it. The eMSP must inform the customer about the renewal and why it's necessary. Reasons for renewal may include (but are not limited to): • PCID renewal from the OEM, • User extending the contract with the eMSP for that specific EV, • Renewal due to technical needs, to keep the contract certificate valid, • Renewal due to technical needs, to update algorithms or cryptographic parameters in line with standards updates. • [Additional control only (see §5)] The customer choosing to add additional authorization for the use of the contract certificate for a specific car (or to remove that additional authorization)
Actors involved	eMSP customer, eMSP
Sequence and interface/ Communication channel	The process varies depending on the cause of the renewal: • If a user requests it (e.g. contract extension), no checks are necessary. • For automatic renewals, eMSP checks opt-in/opt-out preferences for contract certificate renewal. eMSP accesses the Provisioning Vehicle Certificate using the PCID in two ways: • By requesting it from the OEM (since the PCID contains an ID of the OEM). • By accessing the corresponding PCP Regardless of the method, the eMSP should inform the user about the need for a new contract certificate. This requires activating the installation on the EV. Finally, the eMSP creates the Contract Certificate and signs it.

Precondition/ Requirements	The customer maintains a valid relationship with the eMSP, has a mobility contract, and at least one EV registered for the PnC service. Moreover, a contract certificate has been issued for that EV.
Postcondition	The contract certificate is generated and the eMSP needs to request publication by a CPS.
Remarks	The renewal of contract certificates should be based on the same mechanisms as the initial installation. According to CharIN alignment for Root-CA's, the CA's responsibility is only to publish new certificates to a specified destination (pool/directory). The download or update in end entities is managed by the OEMs of those devices

1.2.6. CCP cleanup

Objective	Keep the published contract certificate bundles up to date and remove expired bundles and those containing revoked certificates.
Short description	The usage of the PnC service depends on a valid contract certificate being stored in the EV. This certificate can be obtained from the CCP during the charging process. To avoid attempts at installing expired or revoked contract certificates, it is essential for the pool to regularly verify the validity of the information it publishes.
Actors involved	CCP
Sequence and interface/ Communication channel	The pool must check the certificate bundles it publishes for the following conditions: • The contained contract certificate is identified as revoked, • The contract certificate's signature has reached its end of validity, • The contract certificate bundle signature is not valid anymore (e.g.: the signature certificate has been revoked). If any of these conditions are met, the certificate bundle should be removed from the pool.
Precondition/ Requirements	The CCP should have the capacity to verify the revocation of contract certificates against the SubCA that generated them, or the OCSP service. Additionally, the CCP should be able to validate the revocation of signature certificates used to sign all certificate bundles in the pool.
Postcondition	Expired or invalid certificates should not be kept in the pool or used for a charging station installation request.
Remarks	The certificate's metadata in the pools can include vital information such as the issuer's name, the contract certificate's serial number, and the signature certificate's issuer. This information can expedite verifications.

1.3. Installation of contract certificate on the EV

This catalogue of use cases outlines the process of installing a Signed Contract Certificate Bundle onto the target EV. It explores 2 installation channels: one through the OEM using its proprietary connection backchannel to the EV, and the other through the EVSE during charging.

The subprocess involves several actors:

- EV,
- eMSP,
- OEM,
- CCP

The following asynchronous processes facilitate certificate provisioning:

- 1.3.1 Retrieval of the Signed Contract Certificate Bundle (SCCB) through the OEM backend.
- 1.3.2 Installation of the contract certificate on the EV through the EVSE (single EMAID per PCID)

All these use cases require the presence of a valid SCCB in a CCP, as outlined in the use cases in chapter 1.2. Since the installation should be verified on the EV, it also requires the EV to have the necessary certificates set up as per the use cases in chapter 1.1.

[Informative] Authorization of use for Contract Certificates

Currently, once an eMSP customer has signed a contract and enabled it for a specific EV, they have no further control over the rest of the process, in their role as an eMSP customer.

The relevant use cases are described in this chapter (installation of the contract certificate into the EV §1.3.1 and §1.3.2 as well as in §4.1.2 and §4.1.3 which contain implementation recommendations for the OEM regarding the management of certificates).

Authorization of use is only an issue if the eMSP customer is different from both the EV-owner and EV driver. §4.1.3 states that the EV user can view all contract certificates linked to the car and choose which to install and use.

However, these operations should be submitted to eMSP customer consent since the subsequent charging session will be billed directly to their account without further interactions.

There are currently no defined use cases requiring eMSP customer consent for the following use cases:

- Contract certificate installation into the car (§1.3.1 and §1.3.2). The initial registration of an EV into the e-mobility contract could include this consent.
- Selection of the contract certificate to use by a selected EV-User (§4.1.3). The eMSP customer is not consulted, informed, or prompted when the contract certificate is selected for use by an EV-user. Furthermore, this use case is included in the OEM HMI, with no delegation of authorization to a third-party (which could be the eMSP or the CCP).

- Charging while using the contract certificate (§2.1). By design, there should be no interaction during this process to make it easier for the EV-user. Since payment is involved, it is expected by the eMSP customer (who is the payer) to control who is currently using their contract certificate.

A note back to this warning is added to §4.1.3. However, there is no definitive requirement in this document to enforce eMSP customer authorization while handling contract certificates in the EV.

Solutions are discussed in §5.

1.3.1. Retrieval of the signed contract certificate bundle (SCCB) through the OEM backend.

Objective	Get the Contract certificate installed into the EV using means provided by the OEM-IT backend.
Short description	The CCP shares the certificate installation response (e.g., at request of the EV OEM) with the OEM's backend, which then forwards it to the contract holder's EV.
Actors involved	CCP, OEM, EV
Sequence and interface/ Communication channel	The OEM is notified about the availability of a new SCCB. The OEM-IT or EV notifies the EV-User about availability of a new contract certificate and requests approval for installation. Note: It is the responsibility of the OEM to get the approval from the user for SCCB installations. The OEM requests the SCCB. The OEM transmits the SCCB to the EV for installation. The EV authenticates the signature of the bundle. Optionally: The EV checks the signature of the contract certificate. The EV decrypts the private key associated with the contract certificate. The EV stores the contract certificate's private key securely in the EV alongside the contract certificate, including The MSP chain (except the MO Root certificate). The EV or the OEM (App) notifies the EV-User about the successful installation of the Contract Certificate.
Precondition/ Requirements	Storage of the Signed Contract Certificate Bundle in the CCP The connection is established between the EV & OEM backend.
Postcondition	The CPS has sent the certificate installation response to the contract holder's EV via the OEM backend.

1.3.2. Installation of the contract certificate in the EV through the Charging Station

Objective	Install the Contract certificate in the EV through the Charging Station.
Short description	Based on the PCID (or EMAID when updating a stored contract certificate) provided by the EV, the CSO retrieves a SCCB from a CCP and transmits it to the EV through the Charging Station for the installation of the contract certificate and related private key.
Actors involved	EV, Charging Station, CSMS, CCP
Sequence and interface/ Communication channel	The EV requests installation of contract certificates to the Charging Station. The Charging Station requests the CSMS to search for a Signed Contract Certificate Bundle from a CCP with the identifier PCID. The CSMS searches for the CCP likely to store the prepared SCCB for the given PCID, using a Directory Service or another available approach. The CSMS forwards the installation request to the CCP. The CCP checks the authenticity of the request's elements and prepares the SCCB in an EXI format. The CCP should only transmit the SCCB marked as default. The CCP sends the signed bundle to the CSMS. The CSMS forwards the SCCB to the Charging Station. The Charging Station sends it to the EV. The EV authenticates the signature of the bundle. Optionally: the EV checks the signature of the contract certificate. The EV decrypts the private key associated to the contract. The EV stores the private key securely. The EV or OEM (App) notifies the EV-User about the successful installation of the Contract Certificate.
Precondition/ Requirements	Storage of the Signed Contract Certificate Bundle in the CCP.

	The EV supports Contract certificate installation over the Charging Station, and the PnC service is activated. A valid ISO 15118 communication with a Charging Station supporting Contract Certificate installation should be in progress. The Contract certificate installation service is proposed by the Charging Station and selected by the EV.
Postcondition	The Contract certificate and the private key have been authenticated and securely installed in the EV.
Suggested technical solution / req. to ensure interoperability	It is recommended that all Charging Stations support the installation of Contract certificates.

1.4. Provide certificate for PnC in private environment

The objective of this sub-process is to setup an EV with the required certificate to start a charging session with an EVSE in a private environment.

As well as in the public environment, a standardized communication protocol is required in the private environment to enable encrypted communication and transmit charging session messages. To save costs, charging should use the same communication protocol on both public and private infrastructure. However, in the private environment, complexity can be reduced by eliminating the use of OCSP and short-lived certificates, which removes the need for the EVSE to be constantly online.

- The Certificate management in the private environment can be simplified, compared to the public environment.
- In a private environment, it is assumed that the user does not need to be billed or authorized through automated and standard means. The owner of the private environment is responsible for authorization and billing.
- The PKI delivering certificates for the EVSE does not need to comply with requirements for the V2G PKI.
- Certificates' validity periods may be longer than those of EVSE certificates in a public environment.
- The contract certificate sent by the EV for authorization does not need to be validated by the EVSE; the EMAID may still be used for offline authorization against a local whitelist.

Several preconditions must be met to establish a smooth-running sub-process:

- It is assumed that the charging infrastructure is operated in a location where physical access by an EV is restricted and is therefore private.
- The EVSE has its own issuer certificate chain (private environment certificates), which can be sent to the EV in a dedicated "pairing mode" to provide the trusted private environment Root certificate required to establish TLS.

As a post-condition, the following will apply:

- In the private environment, the EV has installed the EVSE issuer certificate (private environment Root Certificate). Contract certificates and OCSP are not used. Otherwise, the charging process remains unchanged compared to charging in public.

1.4.1. Installation of the private operator Root CA certificate in the EV through the Charging Station

Objective	Install the private operator Root CA certificate in the EV through the Charging Station.
Short description	A first-time connected EV to a Private Environment EVSE will activate a "pairing mode" to enable storage of the private operator root certificate shared by the EVSE during the TLS setup.
Actors involved	EV, EVSE
Sequence and interface/ Communication channel	The EV is set into a PE "pairing mode". The EV and EVSE align to set up TLS. The EVSE sends the entire private operator EVSE certificate chain, including the Root CA certificate, to the EV. The EV stores the Root CA certificate. TLS is established. The EV and EVSE can then offer or select "contract-based payment" (PnC) or EIM. In case of "contract-based payment", the EV provides a contract certificate to the EVSE. The EVSE may not validate the certificate if there is no online connection. The EVSE may authorize the EMAID against a local whitelist. In case of EIM, the EVSE user provides authentication, and the EVSE authorizes it.
Precondition/ Requirements	EVSE is located in a private environment EVSE is setup with a private operator certificate chain
Postcondition	The EV is authorized.
Suggested technical solution / req. to ensure interoperability	As a recommendation, the pairing mode might be established by a push-button function at EV side.

2. Use PnC contract certificate

This section describes how certificates are used during charging once the initial setup of all parties is complete, as detailed in previous chapters.

These use cases are initiated automatically when an EV-User plugs in their ISO 15118-compliant vehicle to an ISO 15118-compliant EVSE (charging station). No user input or interaction is required at this point, although each OEM might have different ways to notify the EV-User that charging is in progress.

The main actors involved are:

- OEM,
- EV,
- EV-User,
- EVSE,
- CSO,
- OCSP Responder,
- eMSP,
- CCP

The following asynchronous processes in this chapter allow for certificate provisioning:

- 2.1. Use of the Plug & Charge Contract certificate for authorization during a charging session
  - 2.1.1. Setup of a TLS session to enable the Plug & Charge service
  - 2.1.2. Authenticate the Contract certificate for authorization
  - 2.1.3. Authorization of charge using the Plug & Charge Contract Identifier (EMAID)

To ensure a smooth charging process, several preconditions must be met:

- The use of certificates on the EV side requires these certificates to be generated and/or installed on the EV.
  - Root CA certificates (OEM, V2G, and if necessary, eMSP) need to be set up and published.
  - V2G Root CA certificates must be installed as trust certificates in the EV.
  - The EV provisioning certificate must be installed following 1.1.2 Provision OEM Certificates
- A contract with an eMSP must be signed and activated for this specific EV, resulting in the generation of a contract certificate and an associated Contract Certificate Bundle, which must be signed by a CPS and published.
- The EV-User must activate the PnC feature and choose to use of ISO 15118 authentication. Other authentication methods may be available, but charging with those alternatives does not require the following use cases.

As a result, and postcondition, the vehicle begins charging. Revoked certificates are removed from certificate pools once the EV system is notified. The OEM is responsible for removing revoked contract certificates from the EV when needed.

2.1. Use of the Plug & Charge Contract certificate for authorization during a charging session

Objective	To enable the EV-User and their EV to be authenticated at the charging station using Plug & Charge based on ISO 15118.
Short description	The EV-User plugs the charging cable into the EV and/or EVSE. As the cable is connected, the EV will automatically identify itself to the charging station, get authenticated, and receive authorization to charge its battery.
Actors involved	EV, EV-User, EVSE, CSMS, CCP/CPS provider, PKI, OCSP responder, eMSP backend
Sequence and interface/ Communication channel	This is an overall use case covering all functions of using certificates during the charging session. The session starts when the EV is plugged to an EVSE and should not require additional user interaction. The sequence then follows these steps: • TLS handshake between EV and EVSE: Verification of the SECC leaf certificate and related trust chain (CSO Sub CA 1 and CSO Sub CA 2) against the V2G Root CA certificate. A TLS session is then established between the EV and the EVSE; • Optionally: Installation of a Contract certificate from a CCP through the EVSE; • Verification of the Contract certificate using a challenge sent by the EVSE (req. 899 from ISO 15118-2) from the Charging station (ISO 15118-2 PaymentDetailsReq/Res); • Authorization by the eMSP for payment based on the Contract certificate EMAID. • Start of power delivery during which no further interactions concerning certificates are in progress. This process mainly consists of 3 parts: 1) Authentication process to the EVSE (TLS Server authentication) that requires the EVSE to provide an OCSP “stapled” response for its own certificate: This step is managed by the EVSE;

	2) Validation of the Contract certificate: This step could be managed by the respective CSO; 3) Authorization process based on the EMAID: This step is managed by the eMSP and CSO (synchronously with a "real-time request", or asynchronously based on a "whitelist").
Precondition/ Requirements	Preconditions are described in Chapter 1 and are referenced here. The following PKI use cases must be set up prior to the charging session. • UC 1.1.1.1 Set up a new Root CA and publish the certificates for the PnC service • UC 1.1.2.1 Install EV necessary certificates • UC 1.1.3.1 Install relevant certificates in the EVSE to enable the PnC service • UC 1.1.3.3 Install relevant certificates in the EVSE to enable a secure communication with the CSMS • UC 1.2.4 Store the signed Contract Certificate Bundle in the CCP It is not required that a Contract certificate be already installed in the EV; however, this would trigger the installation of a Contract certificate during the session. Other prerequisites: There is a roaming agreement between the eMSP and the Charge Point Operator.
Postcondition	The EV-User has successfully started the charging transaction using Plug & Charge based on ISO 15118. The charging operation begins has and should be visible to the EV-User through lights or a display. If there's an error, an indication is sent back and displayed to the user. The onboard display is the responsibility of the OEM. The charging station can also display the session status to the user. Error indications may be shown by the charging station but are not required.
Suggested technical solution / req. to ensure interoperability	Charging Station certificate authentication validation: The charging station must present its full chain up to, but excluding, a Root CA certificate recognized by the vehicle: • either containing multiple Cross Certification: certification path shall not exceed 4 levels

	• or with a Certificate Trust List (CTL): the EV should handle up to 5 V2G Root certificates, as recommended in the ISO15118-2 specification. Verification of revocation is required (using OCSP Stapling). Authorization: Challenge authentication for the contract certificate is required by V2G2-901 from ISO 15118-2. Contract Certificate authentication: The CSO should check the full chain, even if the contract certificate does not contain the full chain. ISO 15118-2 requests the EV to send the full contract certificate chain. The CSO must ensure this verification is done, preferably as early as possible, to terminate invalid authorization requests promptly: • Verification by the charging station requires that all SubCA are present on the charging station. The charging station then contacts the CSMS. The CSMS should be able to require authorization for the correct contract information based on EMAID. The CSMS requests the eMSP for authorization.

2.1.1. Setup of a TLS session to enable the Plug & Charge service

Objective	Authenticate the EV and the EVSE and establish a secure communication channel.
Short description	The EV-User plugs the charging cable into the EV and/or EVSE. As the charging cable is plugged in, the EV will automatically authenticate the charging station. For -20: If the EV is configured accordingly, the EVSE will authenticate the EV as well.
Actors involved	EV, EVSE, OEM OCSP Responder (For –20 only)
Sequence and interface/ Communication channel	When plugged in, the EV initiates the connection to the EVSE following the TLS protocol: • TLS 1.2 (or later versions) protocol is to be used. • The EV asks the EVSE to establish secure communication, sharing its supported Root CAs. • The EVSE responds with its SECC leaf certificate, certificate chain, and Sub-CA certificates' OCSP status. The EV validates the certificate by checking the entire certificate chain and the OCSP status. • EV and EVSE negotiate for the cipherSuite they will use. Both EV and EVSE must support cipherSuites specified in ISO 15118-2. Both EV and EVSE generate the same master key and derived keys to encrypt and authenticate records.
Precondition/ Requirements	The V2G Root Certificate is installed in the EV. The EVSE is setup for ISO 15118 authentication. • It has obtained a SECC certificate and own the matching private key, which must be securely stored. • It contains the certification chain of its own SECC certificates, up to the matching Root CA. The EVSE has obtained a valid OCSP status response for each of its CSO Sub CA certificates.
Postcondition	Transport & security layers are ready for PnC charging operations.

	An indicator should show that charging session is in progress. In case of an error, an indicator should show that the charging session could not start. Additional detailed information might be available to the EV-User at the discretion of the EV OEM and CPO.
Suggested technical solution / req. to ensure interoperability	Use-case on Trusted List of Root-CAs vs. Cross-Certification. To ensure interoperability, ISO 15118-2 requires the EV to handle a trust list of up to 5 V2G Root certificates. Cross-certification may be more complex. The trust list seems like a better solution but is still under discussion at the ecosystem level.
Remarks	Charging Station certificate authentication validation: The charging station should present its full chain up to, but excluding, a root recognized by the vehicle: • either containing Cross Certification or • with a Trust List Verification of revocation status is required (using OCSP).

2.1.2. Authenticate the contract certificate to use for authorization

Objective	The EV authenticates using its contract certificate to confirm possession of a valid certificate and associated private key.
Short description	The EV requests the ISO 15118 authorization challenge. It presents its chosen contract certificate, the EMAID, and the response to a challenge to ensure proof of possession of the private key. The charging station verifies the certificate's validity and the challenge response
Actors involved	EV, EVSE, OCSP Responder
Sequence and interface/ Communication channel	1. The EV first presents the contract certificate and Sub-CA chain (with the PaymentDetailsRequest). 2. The EVSE sends the (PaymentDetailsRes with the) challenge. 3. The EV sends the (AuthorizationRequest containing that) same challenge, signed with the private key corresponding to the contract certificate. 4. The EVSE verifies the signature of the AuthorizationRequest with the public key of the contract certificate, which it received in the previous PaymentDetailsRequest from the EV. Validation checks of the contract certificate are required either at the EVSE or at the CSMS. It is the responsibility of the CSO to ensure that verification is done. It is recommended that the contract certificate checks are processed as early as possible, preferably on the EVSE. It is recommended that a revocation check is also performed during certificate validation. However, in the case of an offline charging station, this revocation check may not be possible. The decision to implement the revocation check is left to the CSO, who will also be responsible for any misuse of a certificate.
Precondition/ Requirements	The contract certificate is installed in the EV. The secure communication between the EV and EVSE has been established. The possible trusted eMSP Roots are installed on the EVSE and/or on CSMS.
Postcondition	The contract certificate is verified by the EVSE or CSMS. The EVSE has obtained the EMAID to request payment authorization

Suggested technical solution / req. to ensure interoperability	Contract Certificate authentication: The EVSE or CSMS should check the full chain, even if the contract certificate does not contain the full chain. All Root CA certificates may be present on the EVSE or CSMS.

2.1.3. Authorization of charge using the Plug & Charge Contract Identifier (EMAID)

Objective	Obtain authorization for payment as a prerequisite to start energy charging, when the charging station is online.
Short description	After secure communication between the EV and EVSE has been established and the contract certificate has been verified, the EVSE or CSMS obtains authorization to start the charge.
Actors involved	EVSE, CSMS
Sequence and interface/ Communication channel	The EVSE requests authorization from the CSMS based on the contract certificate and EMAID. The CSMS requests payment authorization from the eMSP. The CSMS validates authorization and notifies the charging station to initiate the charge.
Precondition/ Requirements	The contract certificate is installed in the car The contract certificate is valid The EMAID has been obtained from the EV / Contract Certificate The CSMS has a method to secure communications with the eMSP.
Postcondition	Authorization has been granted and transmitted to the charging station. Charging begins.
Suggested technical solution / req. to ensure interoperability	Secure communication should be available to allow payment authorization communication.
Remarks	The secure communication, direct or indirect, between the CSMS and the eMSP has been identified. Certificates used for that secure communication are not currently described in ISO 15118 PKI uses. They are, however, required for the charging process. An additional use of the PKI may be defined, or other TLS certificates may be used for that purpose.

3. Crypto-agility

Crypto-agility is a safety measure or incident response that aims to design information security protocols and standards to support multiple cryptographic primitives and algorithms simultaneously. Its primary goal is to enable rapid adaptation of new cryptographic primitives and algorithms without making disruptive changes to the system's infrastructure. This document shares a small set of recommended practices to help hardware manufacturers implement crypto-agility, even though it is not yet required.

3.1. Crypto-agility applied to PnC

In the ISO 15118-2 standard, there is no mention of crypto-agility support. Therefore, a system can be declared as conforming to ISO 15118-2 requirements even if it does not support any built-in crypto-agility concepts. Nevertheless, it is strongly recommended to plan for an agile design regarding cryptography modules in current system developments. This will enable a future forward compatibility on the hardware side.

The introduction of a new Crypto Suite, new algorithms, and extended key length must be well prepared. Since it will lead to incompatibilities if only one system supports the new algorithms and other systems don't, changes always must be implemented backward compatible.

Three options to update V2G entities' Crypto Suite/new algorithms:

- Suite update via flash update in service/garage
- Online update via OEM FOTA Services
- For EV only: Online update via charging infrastructure (value-added services)

3.2. Recommended practices

Design recommendations

- Define handling of "legacy" data after updates (revocation and re-signing or valid until expiry, handling of legacy devices)
- Check IT system designs (backend) to support crypto agility (e.g., no fixed length for data structures that include crypto) - reviewed and recommended.
- Define allowed overlap / transition handling for backward compatibility during algorithm change phases.
- In case of critical incidents / exploits, it is recommended to have an online update mechanism in place, as the cipher suite needs periodic updates to ensure security.
- Ensure continuous evaluation of the security level of available algorithms

Technical implementation recommendations

- Enable Cipher Suites (software libraries / hardware implementations of cryptographic algorithms) and credentials (cryptographic keys, certificates) to be updated during the lifetime of a V2G entity,

either to address incidents or exploits in existing libraries or to roll out new cryptographic algorithms.
    - The Cipher Suite is a security relevant component; therefore, the update must be secured against manipulation. Trust anchors must be available in the system, with backward compatibility, for a defined time slot to ensure secure updates.
- Check communication protocols to support crypto agility (e.g., predefined curves in ISO15118-20, by Algorithm IDs or Algorithm negotiation) reviewed, recommended
- Plan for hardware support of future evaluations and requirements

The technical realization of cipher suite updates for a specific entity (EV, Backend System, CA, etc.) is the responsibility of the actor providing the V2G entity.

4. Implementation recommendations for specific actors

This chapter summarizes recommendations for the OEM and eMSP regarding use cases where the actual sequence and implementation are left to their discretion. If these recommendations are considered early in the process, they will help stakeholders in the Plug & Charge ecosystem set up a robust and efficient system, aiming to provide the best possible user experience.

Below are the functionalities concerned by these recommendations:

- 4.1. OEM specific recommendations
  - 4.1.1. Activation or deactivation of the Plug & Charge feature from the electric vehicle
  - 4.1.2. Activation or deactivation of the Contract certificate installation request from the electric vehicle
  - 4.1.3. Managing Contract certificates from the electric vehicle
  - 4.1.4. Ensure the PCID is used by authorized persons from the OEM perspective
- 4.2. eMSP specific recommendations
  - 4.2.1. Ensure the PCID is used by authorized persons from the eMSP perspective
  - 4.2.2. Unsubscribe from the e-mobility service of an eMSP
  - 4.2.3. Termination of an e-mobility contract

As a recommendation for EVSE, if the charging station detects an EIM before starting the payment method sequence from ISO 15118-2, the charging station should use the EIM and refuse the Plug & Charge authentication means.

4.1. OEM specific recommendations

This section summarizes OEM-specific recommendations that meet user and safety needs. Their implementation depends on the technical choices of the OEM but aims to offer similar operation between systems to promote the adoption of electric vehicles by improving the user experience.

4.1.1. Activation or deactivation of the Plug & Charge feature from the electric vehicle

Objective	Allow the EV-User to choose their means of identification and payment for each charging session individually (e.g., e-mobility contract subscribed to an eMSP: RFID or Contract certificate, credit card, cash, etc.). The solution must allow the Plug & Charge function of the EV to be deactivated and reactivated.
Short description	The EV-User activates or deactivates the Plug & Charge feature of their vehicle (e.g.: from the HMI of the vehicle, or from the OEM application). This allows other users of the vehicle to identify themselves and pay by their preferred method to use the charging service.
Actors involved	EV-User, EV
Sequence and interface/ Communication channel	1. The EV-User navigates in their user settings from the HMI of the electric vehicle or from the OEM mobile application and selects their means of identification. 2. The EVCC uses the last setting selected by the user for the next charging session.
Precondition/ Requirements	The OEM allows the EV-User to adjust their user settings related to identification methods: • The electric vehicle has all the necessary prerequisites for using the Plug & Charge feature; • The Plug & Charge feature can be easily deactivated temporarily until reactivated by the EV-User; • The EV-User has access to an interface: (e.g., HMI of the electric vehicle or OEM application), to perform this operation. The user preference must be set before plugging the electric vehicle into the charging station.
Postcondition	While the Plug & Charge feature is deactivated by the EV-User, the EVCC shall use the EIM for identification to the charging station. While the Plug & Charge feature is activated by the EV-User, the EVCC shall request the Plug & Charge identification with the Contract certificate to the charging station.
Suggested technical solution / req. to ensure interoperability	User preference can be defined in the user settings from the HMI of the electric vehicle or from the OEM application.
Remarks	This choice is left to the user at any point before beginning charging. The activation / deactivation process should not take more than a few seconds. No changes can be made to the electric vehicle after plugging in.

4.1.2. Activation or deactivation of the Contract certificate installation request from the electric vehicle

Objective	The EV-User can activate or deactivate the installation request for specific Contract certificates from the charging station via the user interface.
Short description	The Plug & Charge feature allows the installation of Contract certificates by the OEM back-end or the charging station. When the user wants to install a specific contract, they can request installation via the charging station. In this case, the vehicle must send the "CertificateInstallationReq" request according to the ISO 15118-2 specification for the charging station to retrieve the available Contract certificate from a secondary actor, like a CCP. The EV-User needs to activate the installation mode in the electric vehicle to send this message.
Actors involved	EV-User, EV (OEM)
Sequence and interface/ Communication channel	1. The EV-User activates the Contract certificate installation mode from the user interface (e.g., HMI of the electric vehicle or OEM application). 2. When initializing communication with the charging station, the electric vehicle sends the "CertificateInstallationReq" message to request installation of the Contract certificate.
Precondition/ Requirements	The Plug & Charge feature is activated in the electric vehicle.
Postcondition	The electric vehicle is enabled to install a new Contract certificate through the charging station.
Suggested technical solution / req. to ensure interoperability	None, the implementation is OEM specific.

4.1.3. Managing Contract certificates from the electric vehicle

Objective	The EV-User can manage their Contract certificates from their OEM application or the vehicle interface (installation and uninstallation from the vehicle). They can select the Contract certificate to activate for the next charging service.
Short description	The eMSP customer has subscribed to one or more e-mobility contracts. In their personal settings (from the OEM application or the electric vehicle), the user selects a default contract. The related Contract certificate and private key must be installed in the electric vehicle to be presented to the station during the upcoming charging session. The user may request the installation or uninstallation of other e-mobility contracts from the OEM application or the electric vehicle. Consequently, the user must be able to change their default contract easily, for example, due to price differences or the use of company or rental vehicles. If additional authorization is required for a specific contract certificate, choosing a contract certificate for payment should be subject to an authorization check that requires confirmation by the eMSP customer.
Actors involved	EV-User, EV, OEM
Sequence and interface/ Communication channel	**The sequence needs to be defined by the OEM. The following statements are requirements:** The EV-User should be able to get a list of all the Contract Certificates installed in the EV that they are authorized to use. The EV-User should be able to select one Contract Certificate they are authorized to use as the default for the next charging sessions. If that Contract Certificate requires additional authorization, the eMSP customer should be notified and required to approve or reject that action. The use of the certificate by the EV-User should be constrained by that authorization. The EV should provide information to the EV-User about the Contract Certificate used for the next charging session. For the installation of a new Contract certificate, the EV should ensure that the EV-User is authorized to install this certificate.

	The EV-User and the EV-Owner should be able to choose to be notified of any changes on their Contract certificates installed.
Precondition/ Requirements	The EV-User has subscribed to one or more e-mobility contracts. The EV-User has a digital interface (e.g., HMI in the EV or OEM application) allowing them to interact with the electric vehicle settings, particularly switching between e-mobility contracts. The default configuration (activated Contract certificate) is defined before the electric vehicle is plugged in. UC 1.2.3 is executed. The EV-User has not selected any Contract certificate for the charging process or wants to change the selection they have already made.
Postcondition	One or more e-mobility contracts are installed in the electric vehicle. Only one e-mobility contract is set by default by the EV-User. The EV-User gets user-friendly information about which e-mobility contract is active on their digital interface. The EV-User's selection is encrypted to be stored securely in their personal settings and is available in the electric vehicle. The electric vehicle uses the Contract certificate activated by the EV-User (default). Optional: The EV-User may authorize other EV-Users to use their Contract certificate selection.
Suggested technical solution / req. to ensure interoperability	Comply with VDE-AR-E 2801-100-1 §11.2.4 The OEM may implement EV-User profiles. The switching process should only take a few seconds. The configuration is carried out before the vehicle is plugged into the charging station. Access to the list of Contract certificates should be subject to the entry of a password, which must be defined between the user and the eMSP or OEM. A user-friendly OEM application and electric vehicle interface should be implemented.

Remarks	The EV-User should be able to get a list of all the Contract Certificates available in the CCP that they are authorized to use.

4.1.4. Ensure the PCID is used by authorized person from the OEM perspective

Objective	Prevent the misuse of Plug & Charge Contract certificates, especially for car sharing, rentals and fleets.
Short description	**General remark**: The PCID is non-confidential data shared through the PKI of the Plug & Charge ecosystem. The customer of a mobility contract with an eMSP is responsible for linking the correct PCID to their contract. The OEM is responsible for installing only authorized contract certificates. The OEM is interested in preventing the misuse of the PCID (e.g., installing the contract certificate in the electric vehicle without the EV user's permission). This use case is specific to the OEM implementation.
Actors involved	eMSP, eMSP customer, OEM, EV, PCP
Sequence and interface/ Communication channel	-
Precondition/ Requirements	-
Postcondition	-
Suggested technical solution / req. to ensure interoperability	Only approved Contract certificates should be installed in the electric vehicle, i.e., the ones authorized by the EV-Owner or delegates. Potential measures: • The OEM blocks the installation of unauthorized Contract certificates in the electric vehicle. • The OEM provides means to transmit the PCID directly to the eMSP with the permission of the EV-Owner (Authentication framework like Oauth2.0). • The OEM provides the PCID only to authorized entities (e.g., through the OEM application, with PIN authorization in the vehicle dashboard). The OEM provides security measures against the disclosure of the PCID.

Remarks	The eMSP needs to verify that the end customer is authorized to have the eMSP create a Contract Certificate Bundle for this PCID. Requiring the eMSP to verify authorization for its customer (e.g.: by checking the vehicle registration document or similar) is a significant obstacle for activating a mobility contract and therefore not appropriate. The user of the vehicle may not possess and may never possess it. Misuse of the PCID can be avoided directly by the issuing OEM through simpler means, as previously described.

4.2. eMSP specific recommendations

This section offers specific recommendations for managing the end of the mobility contract or the relationship with the eMSP, addressing user and security needs. Implementation depends on the technical choices of the eMSP but aims to propose good practices for coordinated ecosystem management.

4.2.1. Ensure the PCID is used by an authorized person from the eMSP perspective

Objective	Prevent the misuse of the Plug & Charge Contract certificates, especially for car sharing, rental and fleets.
Short description	**General remark**: The PCID is non-confidential data shared through the PKI of the Plug & Charge ecosystem. The customer of a mobility contract with an eMSP is responsible for linking the correct PCID to their contract. The OEM must install only authorized contract certificates. The eMSP needs to ensure the correct PCID is provided by its customer (not misspelled) to link the mobility contract to the intended electric vehicle. This use case is specific to the implementation of the eMSP.
Actors involved	eMSP, eMSP customer, OEM, EV, PCP
Sequence and interface/ Com. channel	-
Precondition/ Requirements	-
Postcondition	-
Suggested technical solution / req. to ensure interoperability	The eMSP ensures that the PCID is correctly submitted by its client (eMSP customer, OEM). Potential measures: • The eMSP provides a way to obtain the PCID from the OEM directly with the EV-owner's permission (Authentication framework like OAuth2.0) • The eMSP provides a way to get the PCID from its client (e.g., OCR, QR-code reader)

Remarks	The eMSP must be able to verify that the end customer is authorized to have the eMSP create a Contract Certificate Bundle for this PCID. Requiring the eMSP to verify authorization for its customer (e.g., by verifying possession of the vehicle registration document or similar) is a significant obstacle for activating a mobility contract and therefore not appropriate. The user of the vehicle may not possess and may never possess it. Misuse of the PCID can be avoided directly by the issuing OEM through simpler means, as previously described.

4.2.2. Unsubscribe PnC certificate for a given EV (PCID)

Objective	The contract certificate becomes invalidated either by the customer for a specific PCID or at the end of the subscription.
Short description	The eMSP customer informs the eMSP to end the validity of the PnC service for a specific electric vehicle (PCID). All PCID-related contract certificates will be revoked and/or deleted.
Actors involved	eMSP customer, eMSP, OEM, EV, CAs (for CRL and OCSP service), CCP, CPS
Sequence and interface/ Communication channel	The eMSP customer informs the eMSP to disconnect the EV from the eMSP contract and end the validity of PnC service for a certain electric vehicle (PCID). The eMSP then informs the respective CAs hosting the CRL and OCSP services about the revocation of the contract certificates. The CAs revoke the contract certificates.
Precondition/ Requirements	The eMSP has created a valid contract certificate for a specific PCID This certificate might already be signed by CPS and stored in the CCP, at the OEM, or in the EV)
Postcondition	The electric vehicle is not able to charge using the contract certificate anymore. CPS, CCP, OEM and EV delete the respective certificates • The revocation status is sent to the electric vehicle by the charging station during the ISO15118 authorization process, OR • The electric vehicle is notified by the OEM back-end that the Contract certificate is revoked.
Suggested technical solution / req. to ensure interoperability	CPS, CCP, OEM, and EV should act immediately once the revocation information is shared. Therefore, they should have a messaging system in place to receive such data in real time.

4.2.3. Termination of an e-mobility contract

Objective	The e-mobility contract ends either with the customer's action or at the end of the subscription.
Short description	The customer ends the e-mobility contract. All related Contract certificates are revoked and/or deleted.
Actors involved	eMSP customer, eMSP, OEM, EV, CAs (for CRL and OCSP service), CCP, CPS
Sequence and interface/ Communication channel	Request for termination of the Plug & Charge service: • The eMSP customer requests the eMSP to terminate the contractual relationship, OR • Once the subscription termination date is reached, the eMSP SubCA adds the Contract certificate associated with the vehicle to its revocation list. The eMSP informs the eMSP customer that the Plug & Charge service will end for all associated vehicles connected to that eMSP relationship. Use Case 4.2.2 applies. The electric vehicle deletes the Contract certificate.
Precondition/ Requirements	The eMSP customer has a valid contractual relationship with the eMSP. The Contract certificate is still valid, OR The Contract certificate is already revoked and deleted.
Postcondition	The Contract certificates are revoked, and the revocation information has been distributed (e.g., CRL/OCSP). The Contract certificates are removed from the electric vehicle and all back-ends (CCP, CPS, OEM, eMSP).
Suggested technical solution / req. to ensure interoperability	The OEM back-end is notified when EV-specific Contract certificates are revoked and automatically removed.

5. Contract certificate additional authorization

This section describes the potential challenges faced by different actors handling contract certificates. This section is for informational purposes only.

5.1. Overview of the actors

Throughout this document, three different human actors have been identified in the handling of the contract certificates:

- eMSP customer: this actor is the customer contracting with the eMSP. He is the actual payer for the charging of one or more EVs defined by him with the eMSP.
- EV-owner: this actor owns the car. He needs to know who is driving his car at all times.
- EV-driver: this actor is the driver.

In most situations, all three roles are played by the same person, and at least the first two are usually the same person. However, these roles can sometimes be distributed among different people.

Balancing the rarity of such situations with the ease of use and seamless usage of Plug and Charge, this document assumes that additional control should be an option for the eMSP customer to activate for a specific contract certificate if needed.

5.2. Overview of the actions that need to be authorized

This document defines the following operations linked to the contract certificate:

Contract certificate:

- Generation at the eMSP
- Signature
- Storage in the CCP
- Listing available contract certificates for installation
- Installation from a contract certificate bundle
- Activation for use in the next charging session
- Use during charging
- Revocation

During generation, the eMSP customers specifies the EV for which this contract certificate is generated but cannot specify the actual EV drivers authorized to use it.

Generation, signature, storage and installation into the EV are consented to when the eMSP customer adds the specific EV to their mobility contract.

Adding an authorization for use is contrary to the idea of transparent PnC without interaction.

Authorization would therefore be required only during activation for use by specific EV drivers.

5.3. Overview of the technical solutions discussed

There are two main technical solutions for managing contract certificates with additional control mechanisms: intrinsic control and interactive authorization. Each solution offers different methods for ensuring that only authorized users can access and use the contract certificates, providing various levels of security and flexibility.

- Intrinsic control: The additional control would be directly tied to the contract certificate. When an EV driver uses a contract certificate with extra control, they may need to enter a specific code inscribed in the contract certificate.
    - Defining and communicating that code would be the eMSP customer's responsibility during generation.
    - The EV software would verify that the entered code matches the one in the contract certificate.
    - This solution means that the control code is fixed for the contract certificate's duration and cannot be changed.
    - Revoking the contract certificate for a specific EV driver requires revoking the contract certificate itself.
- Interactive authorization: This method requires the explicit approval from the eMSP customer. When an EV driver wants to use a contract certificate which is identified as requiring additional control, an authorization request should be sent to the certificate owner.
    - The owner should be identified from the contract certificate information, either by the CCP or the eMSP that issued the contract certificate.
    - The EV software should request authorization.
    - The authorization mechanism should be available on the CCP or eMSP side, allowing them to notify the owner for approval and then send an asynchronous message to the EV with the authorization result.
    - Revoking user access would need additional automatic verifications or notifications between the EV and the CCP or eMSP to inform the EV of the authorization revocation.

6. Conclusion & Next Steps

This guide serves as a base for future developments to ensure interoperability. We recognize that it doesn't cover all market activities, but shout address most use cases. If there are additional, unaddressed use cases, please inform CharIN so they can be included in the next document revision.

Future evolutions and scope considered for the document

The following items are not described in this document and will be integrated into future releases:

- CCB content
- Tariff management
- Handling OCSP verification for offline charging stations
- Selection of Contract certificate when multiple Signed Contract Certificate Bundle available at the CCPs
- Pairing mode in a private environment
- Securing charging station initialization
- Manage customer authorization to use PCID (protect against brute force attacks on eMSP and CCP).

IV References

This document was created by the Task Force PKI of the CharIN association.

Contributing Authors:

- Ronald Heddergott (CARIAD)
- Jean-Marc Rives (Gireve)
- Michel Girier (Gireve)
- Steffen Rhinow (Hubject)
- Alexander Plath (Shell)
- Marc Mültin (Switch)
- Mourad Tiguercha (Vedecom)
- Nicolas Lheraud (Vedecom / Mobena)
- Christoph Paul Albrecht (CharIN)

A Appendix

A.1. Secure Communication with Local CSMS

According to the installation topology, an LCSMS can be installed to fulfill the role of local supervision for charging stations. This LCSMS acts as an intermediary between the charging stations and the remote CSMS. Securing the communication links between the LCSMS, the charging station, and the remote CSMS is necessary. This security is achieved by establishing a TLS tunnel between the components, similar to the link described in the nominal case of the document between the charging station and the remote CSMS.

To facilitate communication between organizations, members of the Mobena project have work to standardize the vocabulary for describing digital certificates used in this context. As a result, the trust chains of certificates implemented are described in the following schema:

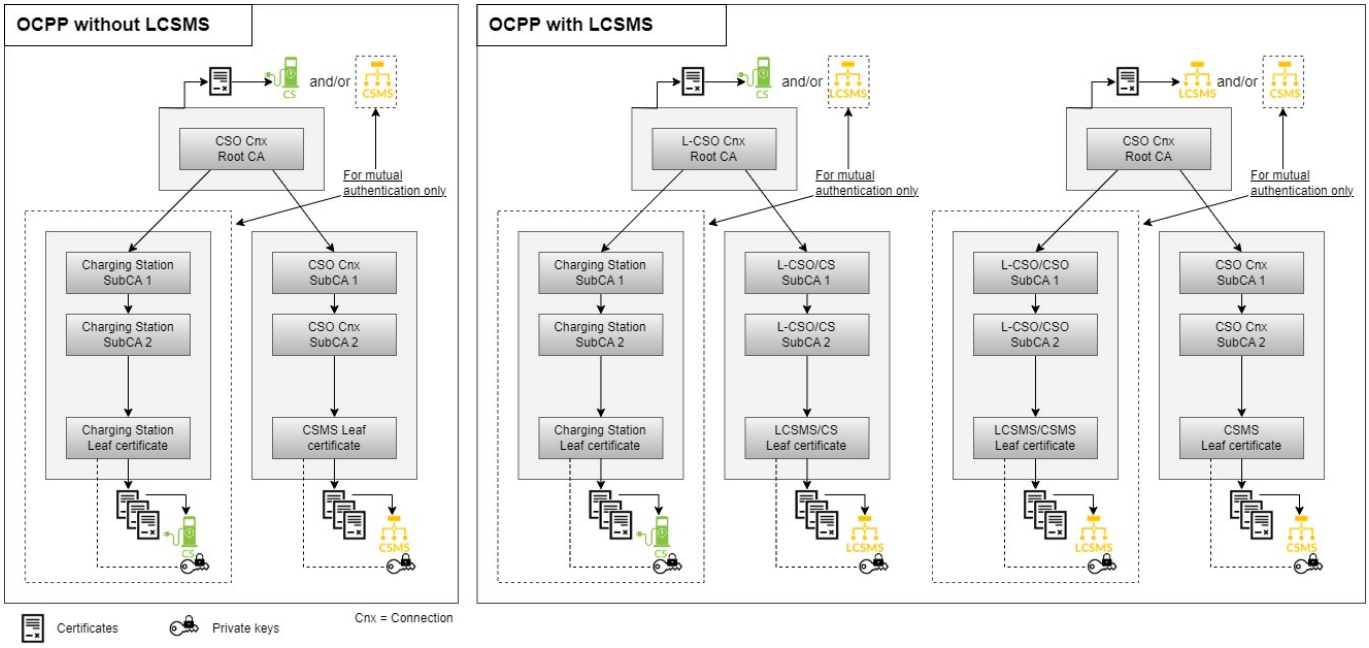


Figure 3: Certificates needed to secure communication in both configurations with and without LCSMS

The certificates installed in the charging station and the remote CSMS remain the same. Only the name of the Root CA changes, but this does not affect the principles of the authentication mechanism. Distinguishing between root certification authorities for the two TLS links allows for a comprehensive description of possible configurations. However, the same authority can be used for both links. Finally, it is important to note that all certificates must adhere to the same standards, regardless of the presence or absence of the LCSMS.

Mutual authentication between the components is not mandatory at present but is highly recommended to ensure optimal system security. Depending on the chosen implementation, the certificates to be installed in the LCSMS are as follows:

	One-way authentication	Mutual authentication (in addition to one-way authentication certificates)
CS – LCSMS	L-CSO / CS SubCA 1 certificate L-CSO / CS SubCA 2 certificate LCSMS / CS Leaf certificate	L-CSO Cnx Root certificate
LCSMS – CSMS	CSO Cnx Root certificate	L-CSO / CSO SubCA 1 certificate L-CSO / CSO SubCA 2 certificate LCSMS/CSMS Leaf certificate