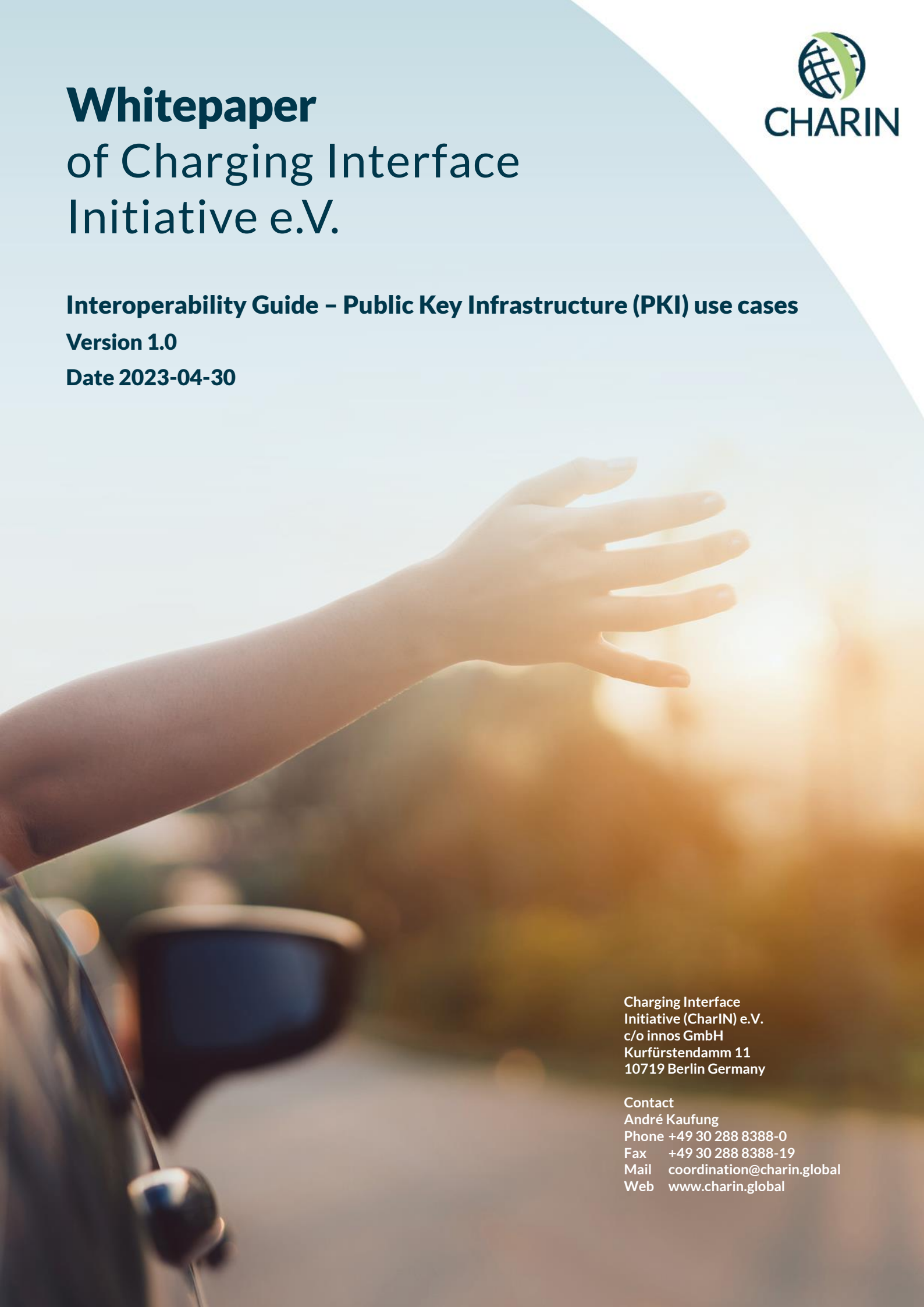


# **Whitepaper** of Charging Interface Initiative e.V.

**Interoperability Guide – Public Key Infrastructure (PKI) use cases**

**Version 1.0**

**Date 2023-04-30**



Charging Interface  
Initiative (CharIN) e.V.  
c/o innos GmbH  
Kurfürstendamm 11  
10719 Berlin Germany

Contact  
André Kaufung  
Phone +49 30 288 8388-0  
Fax +49 30 288 8388-19  
Mail [coordination@charin.global](mailto:coordination@charin.global)  
Web [www.charin.global](http://www.charin.global)

## Contents

1. Introduction .....	3
1.1. Purpose of document .....	3
1.2. Normative references .....	3
1.3. Symbols and abbreviated terms .....	4
2. Provide necessary certificates to operate the Plug & Charge service.....	9
2.1.1. Provide certificates for initial setup of each of the PnC service stakeholders .....	13
2.1.2. Provide Contract Certificates .....	36
2.1.3. Install contract certificate on EV .....	47
2.1.4. Provide certificate for PnC in private environment.....	51
2.2. Use PnC contract certificate.....	54
2.2.1. Use of the Plug & Charge contract certificate for authorization during a charging session.....	56
2.3. Crypto-agility .....	65
2.3.1. Crypto-agility applied to PnC .....	65
2.3.2. Recommended practices .....	65
2.4. Implementation recommendations for specific actors.....	67
2.4.1. OEM specific recommendations.....	67
2.4.2. eMSP specific recommendations .....	75
3. Conclusion & Next Steps .....	79
3.1. Future evolutions and scope considered for the document .....	79
4. Reference .....	80

# 1. Introduction

## 1.1. Purpose of document

The VDE-AR-E 2802-100 defines WHAT the individual roles in the ecosystem must do so that an EV can pick up its contract certificate bundle via the charging station of the CSO or alternatively via the OEM backend and install it for later use. The VDE-AR-E 2802-100 defines that an eMSP must generate a contract certificate bundle and transport it to the store (pool) of the CPS.

The VDE-AR-E 2802-100 provides the functional basis. CharIN must now define the specific implementation and design of the different IT systems so that 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 individual instances should be technically protected
- HOW the security of the individual OSI layers can be achieved on 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.)

Currently the following document uses DIN EN ISO15118-2:2016.

DIN EN ISO15118-2:2022 requirements maybe considered in another version of this document.

Both standards will coexist.

## 1.2. Normative references

The present document refers to the following standards:

- **ISO15118-2**  
Road vehicles – Vehicle-to-Grid Communication Interface  
Part 2: Network and application protocol requirements
- **VDE-AR-E 2802-100**  
Handling of certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO15118
- **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

### 1.3. Symbols and abbreviated terms

<b>CCB</b>	Contract Certificate Bundle	
<b>CCP</b>	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.	
<b>Certification Authority</b>	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
<b>Contract Certificate</b>	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	
<b>CP</b>	Certificate Policy	
<b>CSO</b>	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)
<b>CPS</b>	Certificate Provisioning Service	
<b>CRL</b>	Certificate Revocation List	
<b>CS</b>	Charging Station	
<b>CSMS</b>	Charging Station Management System	CPMS (Charging Point Management System)

<b>CSR</b>	Certificate Signing Request	
<b>Customer</b>	<p>The Customer is the system actor which is the customer of the eMSP who will pay the charging services.</p> <p>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.</p>	
<b>Directory Service</b>	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.	
<b>eMAID</b>	<p>Electric Mobility Account Identifier</p> <p>This is the identifier of the account that the customer has with its eMSP</p>	
<b>EV</b>	<p>Electric Vehicle</p> <p>There is no restriction about the nature of this EV. It could be a car, a bus, a truck, a motorcycle ...</p>	
<b>EV-User</b>	<p>The EV-User is the system actor which uses the EV.</p> <p>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.</p>	
<b>EV-Owner</b>	<p>The EV-Owner is the system actor which has ownership of the EV.</p> <p>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.</p>	
<b>EVSE</b>	<p>Electric Vehicle Supply Equipment</p> <p>The EVSE is the electric part of a charging station that manages the delivery of energy to the vehicle.</p> <p>The Charging Point is the ability of a Charging Station to charge one vehicle at a time.</p> <p>As there is one EVSE per charging Point and one Charging Point per EVSE, both nouns are synonymous.</p>	Charging Point
<b>EVSEID</b>	Electric Vehicle Supply Equipment IDentifier	
<b>HSM</b>	Hardware Security Module	
<b>IT</b>	Information Technology	

<b>Message broker</b>	The message broker is a central message router for all ecosystem participants described in this document	
<b>MO</b>	<p>Mobility Operator</p> <p>The MO is the system actor that offers services to the customers, and typically the EV Charging services.</p> <p>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.</p>	<p>eMSP (Electric Mobility Service Provider)</p> <p>MSP (Mobility Services Provider),</p> <p>EMP (e-Mobility services Provider)</p>
<b>OCPP</b>	Open Charge Point Protocol	
<b>OCSP</b>	Online Certificate Status Protocol	
<b>OCSP Responder</b>	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.	
<b>OCSP Stapling</b>	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.	
<b>OEM</b>	<p>OEM stands for “Original Equipment Manufacturer” which is an ambiguous term.</p> <p>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.</p>	Car Maker
<b>PCID</b>	<p>Provisioning Certificate Identifier</p> <p>The PCID is an identifier of the EV.</p>	
<b>PCP</b>	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.	
<b>PKI</b>	Public Key Infrastructure	
<b>PnC/P&amp;C</b>	Plug&Charge	
<b>Private Environment</b>	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.	
<b>Provisioning Certificate</b>	<p>The provisioning certificate is an X509 certificate that authenticates the EV.</p> <p>This certificate is issued on behalf of the OEM (of the EV) and must be installed in the EV.</p> <p>The Common Name (CN) of this certificate contains the PCID of the EV.</p>	
<b>RCP</b>	<p>Root Certificates Pool</p> <p>RCP is a data exchange and communication facility, on which the asynchronous (and synchronous) exchanges of RootCA Certificates between actors is based.</p>	
<b>RFID</b>	Radio Frequency Identifier	
<b>Root CA</b>	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	
<b>RP</b>	Roaming Platform	
<b>SCCB</b>	Signed Contract Certificate Bundle	
<b>SECC</b>	<p>Supply Equipment Communication Controller</p> <p>The SECC is the ISO15118 communication part of the Charging Station that communicates with the EV.</p> <p>There is only one SECC per Charging Point, but several Charging Point could share the same SECC.</p>	

<b>SECCID</b>	<p>Supply Equipment Communication Controller Identifier</p> <p>This identifier should allow any EV to identify the SECC as a unique entity and check that its authentication certificate matches that SECCID.</p>	CPID (Charge Point Identifier)
<b>SECC Certificate</b>	<p>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 certificate naming. The Common Name (CN) of this certificate contains the SECCID.</p>	EVSE Leaf Certificate, Charging Point Certificate
<b>Sub CA</b>	<p>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.</p>	
<b>Trust List of Root CA</b>	<p>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.</p>	CA TL, TL of RCA, Trust Anchors



## 2. Provide necessary certificates to operate the Plug & Charge service

This chapter will describe all use cases and sub-use cases needed to enable the provision of the operation certificates for the PnC service over all stakeholders. In general, the process of commissioning the certificates of each of the stakeholders is carried out in several stages, some of which run in parallel (asynchronous data flow) between the different roles and their respective communication paths in the ecosystem.

There are different actors involved in the general process: Customer (more precisely the EV-Owner or a person authorized by him), OEM/OEM-Backend, eMSP, PCP, CPS, CCP, CSO, EV, EVSE, RCP.

Within the process several asynchronous sub processes and use cases need to take place in order to allow the provision of the certificates needed for a standardized communication and operation.

- UC1.1: Provide certificates for initial setup of each of the PnC service stakeholders
- UC1.2: Provide Contract Certificates
- UC1.3: Install Contract certificates on EV
- UC1.4: 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 2<sup>nd</sup> 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 following.

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

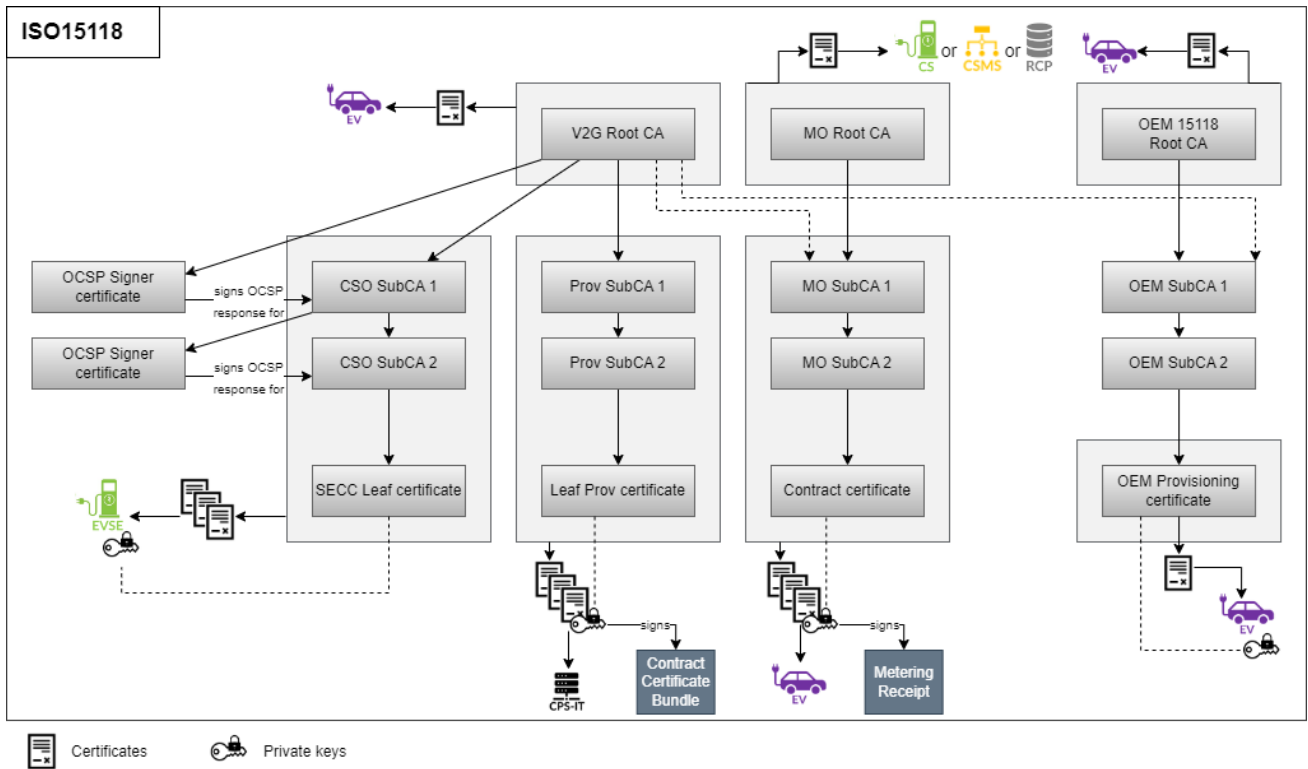


Figure 1: Certificates needed to operate Plug & Charge service

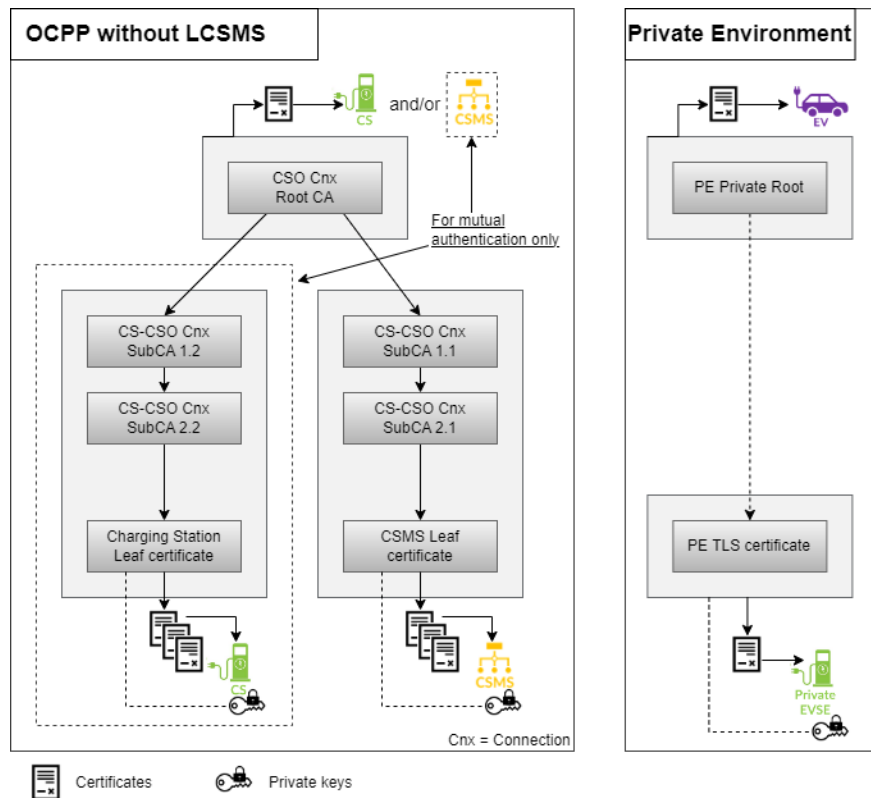


Figure 2: Certificates needed to secure communication between charging station and CSMS, and to operate the service in private environment

The following certificates may be required for the initialization or maintenance of embedded systems by participating in the verification of data transmitted from the cloud; they do not participate directly in the performance of the Plug & Charge service:

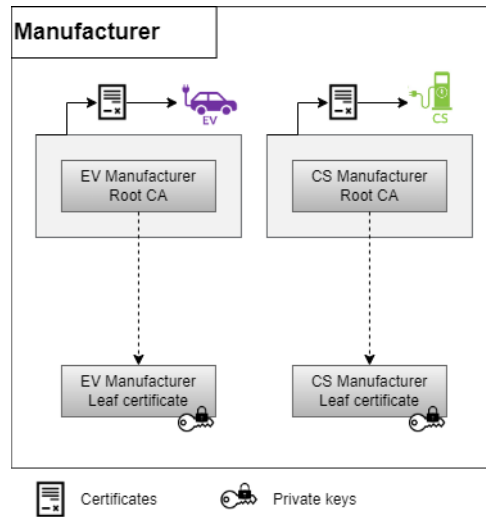


Figure 3: Certificates necessary for the commissioning and maintenance of the service

### **2.1.1. Provide certificates for initial setup of each of the PnC service stakeholders**

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

In general, the process of commissioning the certificates of each of the stakeholders is carried out in several stages, some of which run in parallel (asynchronous data flow) between the different roles and their respective communication paths in the ecosystem to obtain the certificate in the provisioning processes for each of the PnC service stakeholders. Actors involved are: OEM/OEM-Backend, eMSP, PCP, CSO, EV, EVSE, RCP.

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

2.0

## Provide Root CA certificates

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

2.2.1.1.1.2 Renew Root CA certificates

2.2.1.1.1.3 Remove trust in a Root CA certificate

## 2.2.1.1.2 Provide OEM Provisioning certificate

2.2.1.1.2.1 Install EV necessary certificates

2.2.1.1.2.2 Provide EV data to the PCP

2.2.1.1.2.3 Renew OEM provisioning certificate at expiry date

2.2.1.1.2.4 Renew the OEM Provisioning certificate during its validity period

## 2.2.1.1.3 Provide EVSE certificatesProvide EVSE certificates

2.2.1.1.3.1 Install relevant certificates in the EVSE to enable the PnC service

2.2.1.1.3.2 Update EVSE certificates to maintain the PnC in service

## 2.0



Install relevant certificates in the CS to enable a secure communication with the CSMS

#### 2.1.1.1. Provide Root CA certificates

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

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

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

The purpose of the use cases described is to allow all involved stakeholders to gain access to those Root CA certificates, and be able to check and trust Leaf certificates belonging to those Root or subordinate CAs.

Actors involved are: OEMs, eMSPs, V2G Root CAs operator, RCP.



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

<b>Objective</b>	Set up a new Root CA and publish the certificates for the Plug & Charge service
<b>Short description</b>	According to ISO15118-2, every role in the PnC ecosystem may operate a Root CA. Root CA certificates are critical trust anchors. At least one V2G Root CA shall be trusted by the ecosystem to operate the PnC service. OEMs and eMSPs may operate their own PKI. One or multiple RCP (Root Certificate Pool) may be used to provide Root CA certificates in a trusted manner: this option is used in this guide. Root CAs certificates may also be exchanged by other ad hoc secure means.
<b>Actors involved</b>	eMSP, CPS, CSO, OEM-Backend, V2G Root CA Operator, RCP
<b>Sequence and interface/ Communication channel</b>	<ul style="list-style-type: none"> <li>▪ V2G Root CA operator: <ul style="list-style-type: none"> <li>- Implements a V2G Root CA compliant with the requirements described in the Certificate Policy (CP) admitted by the PnC ecosystem stakeholders: CP requirements are set up by CharIN Task Force (<a href="#">link</a>)</li> <li>- Generates a V2G root-CA certificate</li> </ul> </li> <li>▪ OEM and eMSP: <ul style="list-style-type: none"> <li>- Optionally, OEMs and/or eMSPs operate (generate / renew) their own Root CA certificates used for their respective PKIs to issue and sign the OEM Provisioning certificates and the Contract certificates.</li> </ul> </li> <li>▪ RCP operator: <ul style="list-style-type: none"> <li>- Implements a "Trusted Storage Instance for Root CA"</li> <li>- Authenticates and registers parties allowed to operate Root CAs</li> <li>- Receives and renews authentic root certificates generated by authorized parties</li> <li>- Saves authentic Root CAs certificates centrally for read-only access</li> <li>- Distributes and retrieves authentic root certificates to parties from RCP: RCP may implement notification system to inform parties about changes.</li> <li>- Note: For an easy access, the RCP operator may implement a secured API to upload and/or download root certificates.</li> </ul> </li> </ul>
<b>Precondition/ Requirements</b>	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.
<b>Postcondition</b>	<p>At least 1 V2G Root CA is approved by eMSP(s), CPS(s), CSO(s), OEM(s) and operates.</p> <p>Every party in the ecosystem has successfully read each other's Root CA Certificate Policy and Certificate Practice Statement.</p> <p>Every Root CA has:</p> <ul style="list-style-type: none"> <li>- Authenticated and registered to the RCP</li> <li>- Issued / renewed a valid Root CA certificate for itself and make it available by depositing it on the RCP</li> </ul>
<b>Remarks</b>	<p>If an OEM/CSO decides to trust a new PKI actor not present in RCP, it is up to him to setup a process and exchange public key certificates.</p> <p>For a generic process we recommend that the new PKI is checked against the CharIn CP, and afterwards the new Root Certificates are published in RCP.</p>

### 2.1.1.1.2. Renew Root CA certificates

<b>Objective</b>	Secure renewal of the trust anchor (Root CA certificate)
<b>Short description</b>	<p>Root CA certificates have to be renewed:</p> <ul style="list-style-type: none"> <li>- At the end of the validity period</li> <li>- When certain attributes are modified (e.g. DN)</li> </ul> <p>This use case describes the regular renewal of a Root CA certificate while it is not compromised.</p> <p>Renewal of a Root CA certificate under compromission is described in UC1.1.1.3 Remove trust from a Root CA certificate.</p>
<b>Actors involved</b>	OEM Backend, CSO, EVSE, eMSP, CPS, RCP
<b>Sequence and interface/ Communication channel</b>	<p>The renewal of the Root CA certificate is highly dependent of the technical implementation of the Root CA storage. The renewal operation can be:</p> <ul style="list-style-type: none"> <li>- Manual update by authorized process/person (e.g. USB-stick)</li> <li>- Online update thought RCP API</li> </ul> <p>If there is a change in the Root CA keys:</p> <ul style="list-style-type: none"> <li>- Resign or renew the Sub-CAs certificates</li> </ul> <p>Make available the new Root CA certificate by publishing it on the RCP.</p> <p>Optionally: Notify the relevant actors of the ecosystem.</p> <p>Retrieve the new Root CA certificates for distribution by every stakeholder (OEM/CSO) to the leaf devices (EV, EVSE, CSMS).</p>
<b>Precondition/ Requirements</b>	Existing valid Root CA certificate available in the RCP
<b>Postcondition</b>	New Root CA certificate published in the RCP
<b>Remarks</b>	Each item a SubCA has signed has to be renewed. The CA is only responsible for publishing new certificates to the defined destination (e.g., pool, directory). The actors (e.g., CSOs, OEMs) are responsible to download/update those certificates into their devices (e.g., EVs, Charging Stations).

The renewal process of a Root CA is generally a long-lasting process, where the old and new Root CA certificates stay valid for a long time. During that process, the old Root CA certificate must never be used for signing new certificates but must stay valid for validity checks.

### 2.1.1.1.3. Remove trust in a Root CA certificate

<b>Objective</b>	<p>If a Root-CA certificate has been compromised, trusted “third parties” (e.g. CSO, eMSP, OEM, CPS) must “indirectly” inform the participants about the compromised Root-CA certificate (and possibly any subordinate CAs) and remove leaf certificates. from interim storage, to be more precise</p> <ul style="list-style-type: none"> <li>- Remove the compromised Root-CA certificate from the RCP</li> <li>- Remove all other affected certificates and signed content (such as cached OCSP responses or CRLs) issued under the compromised Root-CA.</li> </ul>
<b>Short description</b>	<p>Normally, everyone involved has a self-interest or, even better, an obligation to check the trustworthiness of the leaf and CA certificates used. Certificates used are no longer trustworthy if the verification of their content such as validity, revocation status or the chain of trust (certificate path) fails.</p> <p>However, if the Root-CA certificate itself is compromised, an automatic check within a PKI becomes difficult since it is the root of the trust chain of this infrastructure. Root-CA certificates of the PKIs required here (e.g. V2G Root-CAs, OEM Root-CAs and eMSP Root-CAs) must therefore be withdrawn from the participant “indirectly” by a “third” trustworthy body. Removing compromised trust anchors themselves mostly requires special manual operations by selected and trusted actors.</p> <p>Such selected and trustworthy actors would be, for example, the operator of a root certificate pool (RCP), a cross-certificate Root-CA or the publisher of a Root-CA trust list.</p> <p>In the event of a compromise, the affected Root-CA operator must notify these actors.</p> <p>These actors must then remove both the corresponding Root-CA certificate from the RCP and the certificates issued under it from other storages.</p>

	<p>This paragraph does not cover all the obligations of the operator of a compromised Root-CA (which falls within the scope of the Certification Policy). However, it outlines a basic procedure that must be followed, such as informing affected participants in the event of a loss of trust e.g. by removing the compromised Root-CA certificates from the RCP.</p>
<p><b>Actors involved</b></p>	<p>Root CA Trust List, Cross-certified Root CA, RCP (Root Certificate Pool), CSOs, eMSPs, OEMs, CPSs</p>
<p><b>Sequence and interface/ Communication channel</b></p>	<p>The sequence begins when the Root-CA operator discovers that its Root-CA's private key has been compromised. the Root-CA operator immediately notifies a few chosen actors that act as relays for the trust Anchor such as:</p> <ul style="list-style-type: none"> <li>- the Root-CA Trust List (if it exists);</li> <li>- other cross-certified Root-CAs (if they exist);</li> <li>- Root Certificate Pools (if they exist).</li> </ul> <p>If a Root-CA certificate is compromised, all certificates issued under that Root-CA immediately lose trust.</p> <p>This affects all sub-CA and leaf certificates issued by this Root-CA, including OCSP responder certificates and CRLs.</p> <p>Basically, there is no longer any trust in this PKI hierarchy. Any OCSP responders are also no longer trustworthy.</p> <p>In order to maintain PKI operation, the entire hierarchy must be rebuilt. This includes the identity (e.g. a new common name) and a new key pair of the Root-CA and all underlying PKI instances such as OCSP responders.</p> <p>It becomes particularly devastating when the signatory of the RCP is himself affected. Then also the RCP or the Certificate Trust List must be set up again.</p> <p>From the updated RCP or Certificate Trust List,</p> <ul style="list-style-type: none"> <li>- The OEM shall remove the Root-CA certificate in the vehicles;</li> <li>- The CSOs shall remove the Root-CA certificate in the charging stations (for verifying contract certificates);</li> <li>- The CPS must recognize the certificates issued by that Root-CA and refuse to deliver contract certificate bundles;</li> <li>- The eMSP must not generate new contract certificate from that compromised Root-CA and should find an alternative Root-CA to deliver them.</li> </ul>

	<p>Unfortunately, once the Root-CA is compromised, charging stations cannot provide reliable proof of certificate revocation status to the EV. In this case, the attacker would probably also falsify the status in the OSCP.</p> <p>The communication must either end the charging station immediately or hope that the compromised Root-CA certificate has been removed from the vehicle by the OEM.</p>
<b>Precondition/ Requirements</b>	<p>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.</p>
<b>Postcondition</b>	<p>The compromised Root-CA certificate has been removed from all directories and caches, e.g. B. the RCP and the Certificate Trust List.</p> <p>All certificates and signed data issued and derived under the Root-CA have been removed from all participants.</p>
<b>Remarks</b>	<p>Immediately after the first notification that the private key of its Root-CA has been compromised, the operator of this PKI must make an accurate assessment of the situation and activities in order to avert damage to its emergency plan.</p> <p>The Root-CA must provide a timeline to achieve normal PKI operation by establishing a new PKI hierarchy.</p>

#### 2.1.1.2. Provide OEM Provisioning certificate

Objective of the sub chapter is to define how the OEM initially provides provisioning and vehicle identities linked to asymmetrical keys generated in the EV and how the OEM renews the key material during the life cycle of the EV.

Actors involved are:

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

#### **Prerequisites:**

The OEM has a registration authority in its IT organization (OEM CA) 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 in its IT organization (OEM CA) that binds these identities to the corresponding public keys for the EV and issues the leaf certificates.

The OEM IT backend has made its OEM Root CA certificate and the OEM Sub CA certificates accessible to eMSPs and the provisioning certificates pool(s) via secure channel.

The OEM can install these leaf certificates automatically in production and in the workshop in the EV hardware as a root-of-trust.

The OEM has the option to automatically renewing these leaf certificates during the life cycle of the electric vehicle via its telematics connection (i.e. over-the-air) and/or in the workshop.

The OEM has registered in its IT organization (OEM CA) the identities necessary for the provision of the contract certificate and the EV's charging infrastructure access.

The OEM has linked these identities to the corresponding public keys for the EV in its IT organization (OEM CA) and issued the leaf certificates.

The OEM has initially automatically saved these leaf certificates in production and in the workshop securely in the EV as a root-of-trust in hardware.

The OEM has automatically renewed these leaf certificates before expiry during the life cycle of the electric vehicle via its telematics connection (i.e. over-the-air) and/or in the workshop.

### 2.1.1.2.1. Install EV necessary certificates

<b>Objective</b>	Preparation of an EV to communicate with the charging infrastructure in accordance with ISO15118-2, during or after EV production process.
<b>Short description</b>	<p>Install all necessary certificates in the EV during or after EV manufacturing:</p> <ul style="list-style-type: none"> <li>- OEM ISO15118 Root certificate;</li> <li>- V2G Root certificate(s);</li> <li>- EV Manufacturer Root certificate(s);</li> <li>- OEM Provisioning certificate and corresponding private key.</li> </ul> <p>Two steps have to be considered in the process:</p> <ul style="list-style-type: none"> <li>- The OEM IT gathers the credentials;</li> <li>- The OEM IT install the credentials in the EV.</li> </ul>
<b>Actors involved</b>	OEM IT, EV, RCP
<b>Sequence and interface/ Communication channel</b>	<p>The OEM IT backend shall ensure the following points:</p> <ul style="list-style-type: none"> <li>- The OEM IT backend and the RCP have authenticated each other and established a connection.</li> <li>- The OEM IT backend transfers its OEM ISO15118 Root CA certificate and optionally OEM sub-CA certificates to the RCP in a secured container via this connection (trust store container defined in VDE-AR-E 2802-100, Appendix C), the RCP validates them and stores them securely.</li> <li>- The OEM IT backend fetches the required V2G Root CA certificates from the RCP and optionally also the PE (private environment) Root CA certificates (see VDE-AR-E 2802-100, 11.2.2) from the RCP in a secured container via this connection (trust store container defined in VDE-AR-E 2802-100, Appendix C), validates them and stores them securely.</li> <li>- The OEM IT backend transfers the OEM ISO15118 Root, V2G Root and EV Manufacturer Root certificates to the EV for installation.</li> <li>- The EV generates (ECU handling the private key) the necessary keys in its secure storage.</li> <li>- The EV establishes a mutually authenticated and secure connection to the OEM IT backend.</li> <li>- The EV requests its individual OEM Provisioning certificate including the OEM SubCA certificates from the OEM IT backend, validates the OEM Provisioning certificate and stores it securely with its private key.</li> </ul>



<b>Precondition/ Requirements</b>	<p>The OEM IT can communicate with the RCP in a mutual authenticated and secure way, which requires both sides having the necessary certificates.</p> <p>The OEM IT operates a certificate issuer instance.</p> <p>The EV can communicate with the OEM IT backend in a mutual authenticated and secure way, which requires both sides having the necessary certificates. This can be achieved by either trust-lists or cross-certification.</p> <p>A PCID is already attributed to the EV.</p> <p>The EV uses secure key storage (Trusted Execution Environment, HSM or Trusted Platform Module 2.0).</p> <p>A recommendation for a secure implementation of the trust store container for root-CA certificates can be found in the VDE-AR-E 2802-100, Appendix C.</p>
<b>Postcondition</b>	<p>The EV has:</p> <ul style="list-style-type: none"> <li>- Registered and authenticated with the OEM IT backend and can communicate mutually authenticated and secure;</li> <li>- Valid OEM ISO15118 Root and EV Manufacturer Root certificates from the OEM are securely stored.</li> <li>- All the relevant V2G Root CA certificates (one at least) are securely stored.</li> <li>- Optional root certification authority certificates from private operators (see VDE AR Appendix C) are securely stored.</li> <li>- The EV individual provisioning certificate issued by the manufacturer and the associated private key is securely stored.</li> </ul>
<b>Remarks</b>	<p>Note: The OEM IT backend should also make its root-CA accessible for other participants (process 1.1.2.2.).</p>

### 2.1.1.2.2. Provide EV data to the PCP

<b>Objective</b>	OEM Provisioning certificate has been generated and is available in PCP.
<b>Short description</b>	EV certificate (OEM Provisioning certificate) is provisioned to the PCP
<b>Actors involved</b>	OEM IT Backend, EV, PCP
<b>Sequence and interface/ Communication channel</b>	<p>The OEM IT Back-end and the PCP establish a secure communication channel.</p> <p>The OEM IT Back-end transmits the OEM provisioning certificate to the PCP (including data containing the V2G Root CA supported by the EV, ISO15118 supported version: XML schema namespace (e.g. “urn:iso:15118:2:2013:MsgDef”), OEM Provisioning certificate chain) to inform about supported ISO-version and EV-HSM support.</p> <p>The PCP stores the certificate and makes it available for relevant parties (e.g. eMSP).</p> <p>If applicable, PCP may provide information about the new EV provisioning certificate package being available.</p>
<b>Precondition/ Requirements</b>	<p>EV is in production phase or already built (part replacement).</p> <p>2.1.1.2.1 Install EV necessary certificates: OEM Root certificate is published in RCP.</p>
<b>Postcondition</b>	OEM Provisioning certificate is created, provisioned to the PCP and made available to eMSPs.
<b>Suggested technical solution / req. to ensure interoperability</b>	<p>Certificate must be ISO15118-2 standard compliant.</p> <p>OEM – PCP communication protocol must be aligned</p>

### 2.1.1.2.3. Renew OEM provisioning certificate at expiry date

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

#### 2.1.1.2.4. Renew the OEM Provisioning certificate during its validity period

<b>Objective</b>	Renewed OEM Provisioning certificate is generated and made available in the EV and to the PCP.
<b>Short description</b>	<p>This use case addresses update of a non-revoked OEM Provisioning certificates during their validity period.</p> <p>Two situations must be considered:</p> <p><u>PCID not changed</u></p> <ul style="list-style-type: none"> <li>- Pros: No change in the identity of the EV, meaning less impact for the end user and the eMSP (PCID/EMAID correspondence).</li> <li>- Cons: Potentially complex initialization process with information from old OEM Provisioning. certificate, delete cached certificates (eMSP /CPS) and any Bundles awaiting installation on EV. If EMAID/Contract certificate are deleted from the EV: restart provisioning and installation with eMSP.</li> </ul> <p><u>New PCID</u></p> <ul style="list-style-type: none"> <li>- Pros: No risk of reusing old OEM Provisioning certificate, simpler initialization procedure, no particular procedure to manage the old OEM Provisioning certificate (cache, bundles...).</li> <li>- Cons: More complex contract certificate installation process, redo everything based on the new PCID with risk of significant impact on the EV-User.</li> </ul>
<b>Actors involved</b>	OEM (EV), PCP, eMSP
<b>Sequence and interface/ Communication channel</b>	<p>The OEM detects the need to update of the OEM Provisioning certificate of an EV.</p> <p>Revoke the previous OEM Provisioning certificate. (This step can be carried out later if the renewal is not related to a security need.)</p> <p>Private/public key pair may be changed by the OEM (or EV).</p> <p>Execute UC 1.1.2.1 Install EV necessary certificates.</p> <p>Execute UC1.1.2.2 Provide EV data to PCP.</p> <p><u>If PCID not changed</u></p>

	<ul style="list-style-type: none"> <li>- The OEM associates the PCID with the new OEM Provisioning certificate;</li> <li>- The OEM notifies eMSP /CPS to delete cached OEM Provisioning certificate and awaiting installation Contract Certificate Bundles of the EV;</li> <li>- If EMAID/Contract certificate are deleted from the EV: The OEM shall request eMSP(s)/CPS to re-provision the contract certificate bundle for installation of contract certificates.</li> </ul> <p><u>In case of new PCID</u></p> <ul style="list-style-type: none"> <li>- OEM gets or creates the new PCID of the EV;</li> <li>- OEM communicates the new PCID to the EV-User;</li> <li>- OEM might add the old PCID to the vehicle data stored in the PCP;</li> <li>- OEM or EV-User (following OEM procedure) informs the eMSP to regenerate a Contract Certificate Bundle for the EV.</li> </ul>
<b>Precondition/ Requirements</b>	Updated OEM Provisioning certificate is not created.
<b>Postcondition</b>	<p>Renewed OEM Provisioning certificate is created, installed in the EV, and made available to eMSPs by provisioning in the PCP.</p> <p>EV ready to install Contract certificates: UC1.3 Install Contract certificate on EV</p>

### 2.1.1.3. Provide EVSE certificates

This sub chapter will describe the responsibilities of the CSO as the EVSEs will be prepared to support the PnC service by the provisioning of the necessary certificates: SECC certificate chains and Root CA certificates.

It only covers the initial commissioning and the updates needed over the time by the CSO.

Actors involved are:

- CSO
- EVSE
- RCP
- OCSP Responder

#### **Prerequisites:**

CSO has registered to or operates a V2G Sub CA to sign SECC leaf certificates and has the means to install certificates at the EVSE or can contract someone to do so.

EVSE provided by 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.

### 2.1.1.3.1. Install relevant certificates in the EVSE to enable the PnC service

<b>Objective</b>	Make the EVSE ready to operate the PnC service
<b>Short description</b>	<p>Making EVSE ready to operate the PnC service means:</p> <ul style="list-style-type: none"> <li>- Managing certificates for both ISO15118 and OCPP communications</li> <li>- Activating both ISO15118 and OCPP communications</li> </ul> <p>To make possible a CSO to prepare a Charging Station to support the PnC service, the manufacturer shall provide a procedure to install the relevant PnC certificates:</p> <ul style="list-style-type: none"> <li>- SECC leaf certificate and related trust chain: required to secure the communication between the Electric Vehicle and the ISO15118-2 communication controller (SECC);</li> <li>- EMSP Root certificates: to authenticate the contract certificates if the contract certificate validation is done by the Charging Station;</li> </ul> <p>Recommended:</p> <ul style="list-style-type: none"> <li>- V2G Root certificate: At least one, trust anchor belonging to the SECC leaf certificate</li> </ul> <p><u>Note:</u> In order to ensure the maintenance of the charging station or to initialize the system in a secure way, the Charging Station manufacturer should install its own CS Manufacturer Root certificate installed during production. This process is not described in this document.</p>
<b>Actors involved</b>	Charging station (EVSE), CSO, Charging Station Management System (CSMS), V2G Root CA/SubCA, RCP, OCSP Responder
<b>Sequence and interface/ Communication channel</b>	<p>The CSMS establishes the communication with the EVSE.</p> <p>The CSMS gets relevant Root Certificates from the RCP (V2G Root and eMSP Root certificate).</p> <p>The CSMS installs EVSE Trust Anchors: V2G Root, eMSP Root and CSO Root certificates depending on the requirements for this specific EVSE.</p> <p>The CSMS requests the EVSE to start Leaf Certificate creation.</p>

	<p>The EVSE generates a new pair of private and public keys.</p> <p>The EVSE generates a CSR (Certificate Signing Request) to be signed by a SubCA of the V2G Root CA. The CSR shall include the SECCID.</p> <p>The EVSE sends the CSR to the CSMS.</p> <p>The CSMS forwards the CSR to the SubCA.</p> <p>The SubCA generates the SECC leaf certificate, signs the certificate and returns it to the CSMS.</p> <p>The CSMS sends the signed certificate (with its related certificate chain) to the EVSE.</p> <p>The EVSE verifies the signed certificate.</p> <p>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).</p> <p>The CSMS requests the OCSP Responder to provide an OCSP response for the SECC Leaf certificate and returns it to the EVSE upon reception.</p> <p>Note: The EVSE shall regularly renew the OCSP response before expiry date (e.g. weekly basis).</p> <p>The CSMS requests the EVSE to activate the PnC service.</p>
<p><b>Precondition/ Requirements</b></p>	<p>The Charging Station (inc. EVSE) supports the PnC service, meaning that ISO15118-2 and OCPP2.0.1 communication protocols are implemented, but the function is not activated.</p> <p>None of the PnC related certificates are installed in the EVSE (i.e. EVSE Leaf, CSO SubCA, V2G Root and eMSP Root certificates), only the EVSE Manufacturer Root certificate.</p> <p>The EVSE and the CSMS have established a trusted and secured communication channel.</p>
<p><b>Postcondition</b></p>	<p>The PnC service is activated in the EVSE: Both ISO15118 and OCPP communications are operational.</p> <p>The required certificates (for instance the eMSP Root and V2G Root CA certificates, and CSO Root certificate) are deployed in charging station.</p>
<p><b>Suggested technical solution / req. to</b></p>	<p>For the optional installation of the CSO Root CA:</p> <ul style="list-style-type: none"> <li>- Better if done by the EVSE manufacturer</li> </ul>



<p><b>ensure interoperability</b></p>	<ul style="list-style-type: none"> <li>- Usage of Registration service (provider by either CSO or EVSE Manufacturer) may be better for operation</li> <li>- Usage of the V2G Root CA may make it easier to manage this provisioning</li> </ul>
---------------------------------------	--

### 2.1.1.3.2. Update EVSE certificates to maintain the PnC in service

<b>Objective</b>	PnC relevant EVSE certificates are up to date.
<b>Short description</b>	<p>The Charging Station or the managing CSMS initiates the certificate update request when it detects that its SECC leaf certificate, V2G Root certificate or eMSP Certificates (if any) are about to reach their expiry date.</p> <p>As a recommendation:</p> <ul style="list-style-type: none"> <li>- Leaf certificate(s) to be updated one week before expiry date</li> <li>- Root certificate(s) to be updated one month before expiry date</li> </ul> <p>Important: The case of revocation of a certificate triggers the update process.</p>
<b>Actors involved</b>	EVSE, CSO, CSMS, Sub-CA/Root CA, RCP
<b>Sequence and interface/ Communication channel</b>	<p>If the certificate to renew is the SECC leaf certificate:</p> <ul style="list-style-type: none"> <li>- Optionally: The EVSE generates a new pair of private/public keys.</li> <li>- The EVSE generates a CSR (Certificate Signing Request) for signature by a SubCA of the V2G Root CA;</li> <li>- The EVSE sends the CSR to the CSMS;</li> <li>- The CSMS forwards the CSR to the SubCA;</li> <li>- The SubCA signs the certificate and returns it to CSMS;</li> <li>- The CSMS sends the signed certificate (inc. the certificate chain) to the EVSE;</li> <li>- The EVSE verifies the signed certificate;</li> <li>- The EVSE requests the OCSP response of the Leaf certificate to the CSMS;</li> <li>- The CSMS requests the OCSP Responder to provide an OCSP response for the SECC leaf certificate and returns it to the EVSE upon reception;</li> <li>- Note: The EVSE shall regularly renew the OCSP response before expiry date.</li> </ul> <p>If the certificate to renew is a Trust Anchor (Root certificate):</p> <ul style="list-style-type: none"> <li>- The EVSE requests the CSMS to renew a Root certificate;</li> <li>- The CSMS gets requested Root certificate(s) from the RCP;</li> <li>- The CSMS forwards the requested Root certificate to the EVSE.</li> </ul>

<p><b>Precondition/ Requirements</b></p>	<p>The EVSE is operating the PnC service.</p> <p>The EVSE and the CSMS have established a trusted and secured communication channel.</p> <p>The EVSE detected a need to update a certificate.</p>
<p><b>Postcondition</b></p>	<p>The EVSE certificates are up to date.</p>

### 2.1.1.3.3. Install relevant certificates in the CS to enable a secure communication with the CSMS

<b>Objective</b>	Prepare the Charging Station to support secure communication with the CSMS, so as to operate the PnC service while respecting cybersecurity requirements.
<b>Short description</b>	This use case describes the security requirements the Charging Station and the CSMS shall implement before operating the PnC service.
<b>Actors involved</b>	CS, CSO, CSMS, CSO Root-CA/Sub-CA, (Charging Station Manufacturer)
<b>Sequence and interface/ Communication channel</b>	<p>The CSO CA (or SubCA) provides a X509 certificate to the CSMS, according to OCPP2.0.1 requirements;</p> <p>At initialization:</p> <ul style="list-style-type: none"> <li>- The CSMS shall authenticate itself by using the CSMS Leaf certificate as server side certificate;</li> <li>- Optionally: In case of client (mutual) authentication, the EVSE shall authenticate itself by using the Charging Station Leaf certificate as client-side certificate.</li> </ul> <p>Verification:</p> <ul style="list-style-type: none"> <li>- The EVSE shall verify the certification path of the CSMS Leaf certificate;</li> <li>- In case of client (mutual) authentication, the CSMS shall verify the certification path of the Charging Station Leaf certificate.</li> </ul> <p>Provide username and password for EVSE to allow authentication to CSMS</p> <ul style="list-style-type: none"> <li>- The user name shall be the Charging Station Identity</li> <li>- The password shall be random</li> <li>- Better if username/password prepared by EVSE Manufacturer</li> <li>- A registration service may be used to update the connection profile of Charging Station before first connection to CSMS</li> </ul>
<b>Precondition/ Requirements</b>	<p>Both of the EVSE and the CSMS supports at least TLS 1.2 version; TLS1.3 or higher versions are recommended;</p> <p>The CSMS is the TLS server and the EVSE the TLS client;</p>

	<p>The CSMS supports TLS with basic authentication (server authentication) or with client-side certificate (server and client authentication)</p> <p>The EVSE supports client-side certificate (server and client authentication)</p> <p>This use case based on OCPP2.0.1 specifications</p> <p>To be state of the art, it is recommended to implement mutual TLS using client-side certificate (server and client authentication).</p> <p>If the EVSE should be configured with a specific CSO Root CA certificate, it needs to be installed prior on the EVSE.</p>
<b>Postcondition</b>	The CSMS and the EVSE prepared to bootstrap a TLS communication

### **2.1.2. Provide Contract Certificates**

The common objective for the use cases in this paragraph is to cover the required operations regarding certificates from the eMSP customer request up to the publication of the Signed Contract Certificate Bundle in a Contract Certificate Pool that can be accessed by OEMs and CSOs for installation in the car.

The underlying use cases describe every step between the subscription to an eMSP, to the delivery of the Contract certificate into the Contract Certificate Pool (CCP) or similar.

Several actors are involved in the subprocess:

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

The following asynchronous processes allows certificate provisioning:

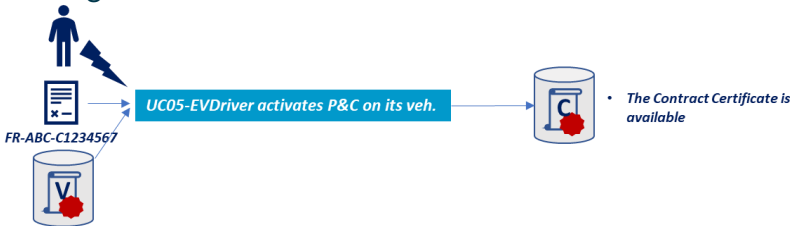
- UC 2.1.2.1 Subscribe to the PnC service: Creation of the Contract certificate
- UC 2.1.2.2 Prepare the Contract Certificate Bundle (CCB)
- UC 2.1.2.3 Sign the Contract Certificate Bundle
- UC 2.1.2.4 Store the Signed Contract Certificate Bundle in the CCP
- UC 2.1.2.5 Renew the Contract certificate from eMSP

These use cases are managed based on the precondition that other players certificates are already set up and ready following paragraph 1.1 use cases. In particular, the EV mentioned in these use cases must have been initialized with a valid Provisioning Certificate, and PKI Services for the RootCa have to be set up for the CPS.

As another condition, the EV-User is required to have subscribed a mobility contract with the eMSP, and that subscription is not described in this document as it does not require the use of certificates.

Finally, the EV-User must have access to the PCID of the EV based on information chosen by the OEM. A list of alternatives is proposed in paragraph 1.2.1, for information purposes only and this list is not exhaustive.

### 2.1.2.1. Subscribe to the PnC service: Creation of Contract certificate

<b>Objective</b>	<p>The eMSP obtains the OEM Provisioning Certificate bound to the target EV, creates a new EMAID if required and generates a Contract Certificate compliant with ISO15118-2 specification.</p>
<b>Short description</b>	<p>The EV-User gets the PCID of the EV via any means provided by the EV-OEM. Some recommended options are listed below.</p> <p>EV-User subscribes to an eMSP with PnC feature support and activates PnC: EV-User must provide PCID of vehicle to the eMSP.</p> <p>After all prerequisite checks, the eMSP:</p> <ul style="list-style-type: none"> <li>- generates an EMAID for the customer (if not yet done),</li> <li>- generates the Contract Certificate</li> </ul> 
<b>Actors involved</b>	<p>EV-User, eMSP, PCP, (OEM), (CPS)</p>
<b>Sequence and interface/ Communication channel</b>	<p>The EV-User initiates the process by requesting activation of PnC feature to its eMSP.</p> <p>The EV-User obtains its PCID; Following options are available (not exhaustive):</p> <ul style="list-style-type: none"> <li>- Common physical ways to exchange digital information, e.g.: smartphone app, vehicle HMI, web interfaces, etc.</li> <li>- Common digital ways to extract information, e.g.: OCR (object character recognition), QR Codes, Authentication Frameworks (OAuth2.0 or similar), etc.</li> <li>- Non-digital solutions could be provided additionally by the OEM as backup-option (not required in case of a pure online relationship)</li> </ul> <p>Based on the strength/weakness analysis below, it is recommended that the customer obtains the PCID as a human (string) and computer (QR) readable code from an HMI (EV, App, etc.) AND/OR an authentication framework with automated data transmission of PCID to the eMSP.</p>

	<p>OEM defines security measures to protect EV from misuse of PCID like unintentional installation of contract certificates: for example, non-activation of any new installed contract certificate at EV before EV-User approval.</p> <ol style="list-style-type: none"> <li>1. The EV-User transmits the PCID of the vehicle to the eMSP. <ul style="list-style-type: none"> <li>– The OEM provides the PCID in a customer friendly way to eMSP customer.</li> <li>– The eMSP customer gets the PCID.</li> </ul> </li> <li>2. The eMSP accesses the Provisioning Vehicle Certificate, using the PCID. <ul style="list-style-type: none"> <li>– By requesting the OEM (PCID contains an ID of the OEM).</li> <li>– By accessing to the corresponding PCP.</li> </ul> </li> <li>3. The eMSP creates the Contract Certificate and signs it. <ul style="list-style-type: none"> <li>– The contract certificate should not have a validity period longer than the remaining validity period of the provisioning certificate for this EV.</li> </ul> </li> </ol>
<p><b>Precondition/ Requirements</b></p>	<p>The eMSP customer takes (delegated) ownership of an electric vehicle and wishes to enable an eMSP contract for that vehicle with PnC and roaming under terms of customer choice. That eMSP contract may be a new or preexisting one.</p> <p>The EV-User has access to the PCID of the related EV.</p> <p>Based on a valid PCID, the eMSP has the ability to identify the OEM or the PCP ready to share the Vehicle Data (EV Provisioning certificate, V2G root ids...), the eMSP may use PCP services for that.</p> <p>The EV-User has a valid subscription to an eMSP service.</p> <p>The vehicle is PnC ISO15118-ready.</p> <p>The EV-User has all the necessary authorizations to activate the PnC service on the related EV.</p>
<p><b>Postcondition</b></p>	<p>The contract certificate is available to be incorporated in a Contract Certificate Bundle.</p>



Note: The following section describes the options an OEM could offer to the customer to retrieve its PCID:

**1) The OEM provides the PCID with the vehicle information sheet.**

– Pros

The PCID is easily made available to the customer.

– Cons

The PCID could change and become outdated, and it could be complicated to get the latest PCID from the OEM. The delivery mean is not secure and require a manual typing of the PCID by the customer to the e-Mobility Service Provider.

**2) The PCID is displayed on the vehicle user interface.**

– Pros

The PCID could be secured by PIN code or other means.

The PCID could be provided using a means familiar to the customer, already used in the telecommunications industry, such as scanning a QR code or entering credentials through an API of a linked account, allowing the chosen solution to be future proof.

– Cons

The customer has to be physically present in the car or using the EV OEM application to get its 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 type of process is not standardized and could lead to multiple possible solutions by OEMs with a high probability of customer friction due to the lack of familiarity by the users (e.g., a dedicated call-center may be necessary).

**4) Implementing an authentication framework allowing the direct supply of the PCID by the OEM to the eMSP**

– Pros

The process can be done outside of the vehicle.

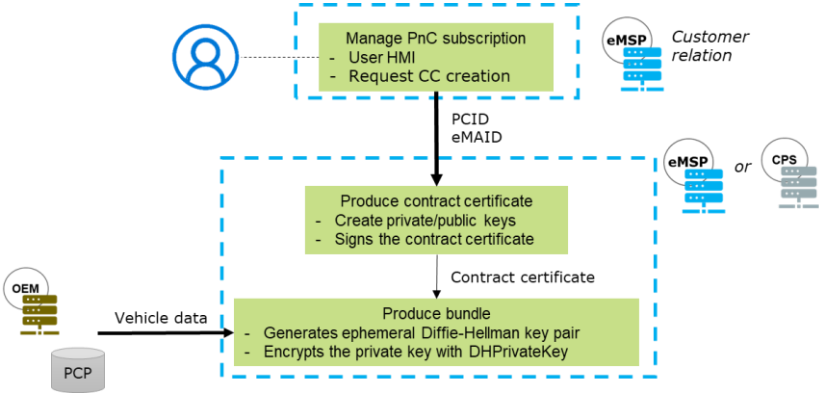
The provisioning process can be fully automated, preventing the user from misspelling the PCID.

– Cons

The customer must have an OEM account.

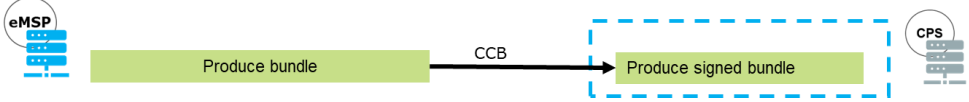
- For some use cases, third party users (non-owners) could require special access to the OEM account with limited access rights (e.g.: for professional purposes such as vehicle fleet manager).

### 2.1.2.2. Prepare the Contract Certificate Bundle (CCB)

<b>Objective</b>	Produce a “ready-to-sign” CCB including the contract certificate, the encrypted private key and vehicle meta-data.
<b>Short description</b>	<p>The UC 1.2.1 handles preparation of the EMAID and the Contract certificate. This use case describes the additional operations necessary to produce the CCB, a self-contained, signed and secure standard package holding necessary elements permitting contract certificate installation.</p>  <p>The diagram illustrates the process of preparing a Contract Certificate Bundle (CCB). It starts with a user (represented by a person icon) interacting with a system to 'Manage PnC subscription', which includes 'User HMI' and 'Request CC creation'. This step is associated with 'eMSP' and 'Customer relation'. The process then moves to 'Produce contract certificate', which involves 'Create private/public keys' and 'Signs the contract certificate'. This step is associated with 'eMSP or CPS'. The final step is 'Produce bundle', which involves 'Generates ephemeral Diffie-Hellman key pair' and 'Encrypts the private key with DHPrivateKey'. This step is associated with 'OEM' and 'PCP'. The flow is indicated by arrows: 'PCID eMAID' from the first step to the second, and 'Contract certificate' from the second to the third. 'Vehicle data' from the 'PCP' is also input to the 'Produce bundle' step.</p>
<b>Actors involved</b>	eMSP, CPS
<b>Sequence and interface/ Communication channel</b>	<p>The eMSP or delegate gets the EV metadata using the PCID contained in the Contract Certificate.</p> <p>The eMSP or delegate generates an ephemeral Diffie-Hellman key pair as specified by ISO15118.</p> <p>The eMSP or delegate encrypts the private key related to the Contract certificate with the Diffie-Hellman private key (generated previously) as specified by ISO15118.</p> <p>The eMSP or delegate gathers every required information into a single CCB object, e.g.:</p> <ul style="list-style-type: none"> <li>- the Contract certificate and related trust chain,</li> <li>- the encrypted private key,</li> <li>- the EV meta data, e.g.: PCID, list of supported V2G RCA, supported versions of ISO15118.</li> </ul> <p>The eMSP or delegate provide the CCB to a CPS for signature (ref. UC 1.2.3).</p>

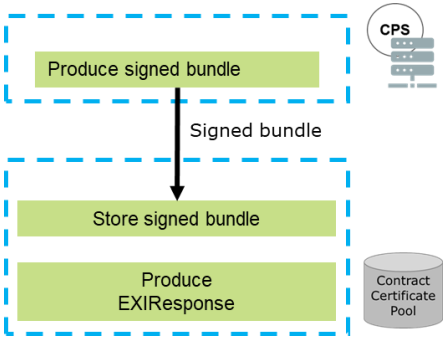
<p><b>Precondition/ Requirements</b></p>	<p>Subscribe to the PnC service: Creation of Contract certificate</p> <p>Based on a valid PCID, the CPS has the ability to identify the OEM or the PCP ready to share the Vehicle Data (EV Provisioning certificate, V2G Root ids...), the CPS may use PCP services for that.</p>
<p><b>Postcondition</b></p>	<p>The CCB is ready to be signed by a CPS.</p>

### 2.1.2.3. Sign the Contract Certificate Bundle

<b>Objective</b>	The Signed Contract Certificate Bundle is made available to be pushed to contract certificate pool (or directly to OEM or CSO).
<b>Short description</b>	<p>The CPS signs the contract certificate bundle (CCB) produced following UC 1.2.2. The signed contract certificate bundle (SCCB) made ready to be provisioned at CCP (or OEM, CSO).</p> <p>If the installed V2G Root CAs at EV side is known, and to ensure compatibility with EV, the signer shall at least have a signing certificate that belongs to one of these supported V2G Root CA.</p> <p>If the installed V2G Root CA are unknown, it is possible to prepare more than one SCCB to cover more than one V2G Root CA and maximize opportunities of compatibility with EV installed V2G Root CAs.</p> 
<b>Actors involved</b>	(eMSP), CPS
<b>Sequence and interface/ Communication channel</b>	<p>Following operations are done by the CPS:</p> <ul style="list-style-type: none"> <li>– If available, gets supported V2G Root CA from the CCB,</li> <li>– Select a signer with signing certificate belonging to supported V2G Root CA scope <ul style="list-style-type: none"> <li>○ If the supported V2G Root CA by EV are unknown, the more likely V2G Root CA is to be targeted, it is also possible to produce multiple SCCB to optimize the chance to have at least one compatible SCCB for contract installation at EV,</li> </ul> </li> <li>– Sign the contract certificate bundle.</li> </ul> <p>The SCCB made ready to be communicated to CCP or directly to OEM or CSO.</p>
<b>Precondition/ Requirements</b>	<p>Prepare the Contract Certificate Bundle (CCB)</p> <p>CCB signer (CPS or eMSP) is a subCA1 or subCA2 of a V2G Root CA likely to be supported by the related EV.</p> <p>Contract certificate bundle is provisioned to CPS.</p>

<b>Postcondition</b>	Signed contract certificate bundle is available to be provisioned to CCP (or directly to OEM/CSO).
----------------------	--

#### 2.1.2.4. Store the Signed Contract Certificate Bundle in the CCP

<b>Objective</b>	Make the SCCB (Signed Contract Certificate Bundle) available at a CCP for installation by the OEM or the CSO.
<b>Short description</b>	<p>After the CCB is signed by the CPS, the SCCB is made available for installation at CCP.</p>  <pre> graph TD     subgraph CPS [CPS]         A[Produce signed bundle]     end     subgraph CCP [Contract Certificate Pool]         B[Store signed bundle]         C[Produce EXIResponse]     end     A -- Signed bundle --&gt; B     B --&gt; C     </pre>
<b>Actors involved</b>	CPS, (eMSP), CCP.
<b>Sequence and interface/ Communication channel</b>	<p>The actor that holds the SCCB (eMSP or CPS) publishes the SCCB at a CCP:</p> <ul style="list-style-type: none"> <li>- The eMSP or CPS establish secured communication with the CCP,</li> <li>- The eMSP or CPS sends the SCCB to the CCP,</li> <li>- The CCP checks the SCCB signature and confirm reception,</li> <li>- If the CCP implements notifications, it notifies subscribers about the new available SCCB.</li> </ul> <p><u>Note:</u> The CCP has to format the SCCB in an EXI format (as specified on ISO15118), if the installation is done by the CSO over ISO15118, the translation to EXI format is done at request reception from CSO as it depends on the ISO15118 communication session information.</p>
<b>Precondition/ Requirements</b>	<p>Sign the Contract Certificate Bundle</p> <p>The eMSP or CPS has already established contractual relationship with at least one CCP.</p>

	<p>eMSP or CPS is able to set a secure communication with the CCP.</p> <p>Recommendations:</p> <ul style="list-style-type: none"> <li>- If multiple CCP available on the market, the CPS has to ensure that the chosen CCP permits distribution of the SCCB to the targeted EV,</li> <li>- To improve interoperability, it is recommended that: <ul style="list-style-type: none"> <li>o CCP operators implements the same APIs</li> <li>o CCP operators organize themselves to be interoperable and cooperative to guaranty SCCB distribution</li> </ul> </li> </ul>
<b>Postcondition</b>	SCCB available for installation by OEM or CSO at CCP.

### 2.1.2.5. Renew the Contract certificate from the eMSP

<b>Objective</b>	Keep the contract certificate up to date to ensure that payment authorizations from the EV are not interrupted due to certificate expiration.
<b>Short description</b>	<p>The usage of the PnC service is bound by the presence of a valid contract certificate stored in the car. The charge point verifies the certificate before charging starts.</p> <p>If this contract certificate has expired charging will be denied. This use case describes the renewal of this contract certificate by the eMSP.</p> <p>The automatic renewal by the eMSP of the contract certificate should be subject to opt-in/opt-out by the eMSP customer while interacting with the eMSP. The eMSP customer should be informed of a renewal and its reasons which can include (not limited to):</p> <ul style="list-style-type: none"> <li>– PCID renewal from the OEM,</li> <li>– Contract extension by the user with the eMSP for that specific EV,</li> <li>– Certificate renewal due to technical needs of keeping the contract certificate valid,</li> <li>– Certificate renewal due to technical needs of updating algorithms or cryptographic parameters to follow standards updates.</li> </ul>
<b>Actors involved</b>	eMSP customer, eMSP
<b>Sequence and interface/ Communication channel</b>	<p>Depending on the cause of the renewal:</p> <ul style="list-style-type: none"> <li>– From a user demand (contract extension), no checks are required</li> <li>– For automatic renewals, eMSP checks opt-in/opt-out options for renewal of the contract certificate</li> </ul> <p>eMSP accesses the Provisioning Vehicle Certificate, using the PCID:</p> <ul style="list-style-type: none"> <li>– By requesting the OEM (PCID contains an ID of the OEM)</li> <li>– By accessing to the corresponding PCP</li> </ul> <p>In all cases, the eMSP should notify the user of the need for a new contract certificate, which requires activation of the installation on the EV.</p> <p>The eMSP creates the Contract Certificate and signs it.</p>

<b>Precondition/ Requirements</b>	The customer has valid relationship with the eMSP and a mobility contract, with at least one EV registered for the PnC service and a contract certificate delivered for that EV.
<b>Postcondition</b>	The contract certificate is generated and the eMSP needs to require publication by a CPS.
<b>Suggested technical solution / req. to ensure interoperability</b>	<p>In Scope:</p> <ul style="list-style-type: none"> <li>– As X.509 v3 certificates are signed data structures, based on a trusted (root) CA, no additional container format is needed for publication,</li> <li>– Requirements for notification of user for the expiry of an installed certificate or contract,</li> <li>– Defined API / Rest-Interface to upload new Certificates into Pool / directory</li> </ul>
<b>Remarks</b>	<p>The renewal of contract certificates should be based on the same mechanisms as the initial installation.</p> <p>Based on the CharIn alignment for Root-CA's, CA only responsible for publishing new certificates to defined destination (pool / directory): download / update in end entities by OEMs of those devices</p>



### **2.1.3. Install contract certificate on EV**

This catalogue of use cases is defining the operation of installation of a Signed Contract Certificate Bundle onto the target EV. It takes into consideration 2 channels for installation: either by the OEM using its proprietary connection backchannel to the EV, or by the EVSE during charge.

Several actors are involved in the subprocess:

- EV,
- eMSP,
- OEM,
- CCP

The following asynchronous processes allows certificate provisioning:

- UC 1.3.1 Retrieve the signed contract certificate bundle (SCCB) through the OEM back-end
- UC 1.3.2 Install contract certificate on EV through EVSE (single EMAID per PCID)

All the use cases require a valid SCCB to be present in a CCP following chapter 1.2 use cases. As the installation should be checked on the EV, it also requires the EV to be set up with the required certificates following chapter 1.1.1 use cases.

### 2.1.3.1. Retrieve the signed contract certificate bundle (SCCB) through the OEM back-end

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

### 2.1.3.2. Install the contract certificate in the EV through the Charging Station

<b>Objective</b>	Install the Contract certificate in the EV through the Charging Station.
<b>Short description</b>	Based on PCID (or EMAID when updating a stored contract certificate) provided by the EV, the CSO retrieves a SCCB from a CCP, transmit it to the EV through the Charging Station for installation of the contract certificate and related private key.
<b>Actors involved</b>	EV, Charging Station, CSMS, CCP
<b>Sequence and interface/ Communication channel</b>	<p>The EV requests installation of certificates to the Charging Station.</p> <p>The Charging Station requests the CSMS to search for a Signed Contract Certificate Bundle from a CCP with the identifier PCID.</p> <p>The CSMS search for CCP likely to store prepared SCCB for the given PCID (using a Directory Service or another available approach).</p> <p>The CSMS forwards the installation request to the CCP.</p> <p>The CCP checks the authenticity of the elements included in the request and prepare the SCCB in an EXI format. In the case where multiple SCCBs are available for the given PCID, the CCP shall identify the SCCBs containing a valid Contract Certificate, and only transmit the most recent among those found.</p> <p>The CCP sends the signed bundle to the CSMS.</p> <p>The CSMS forwards the SCCB to the Charging Station.</p> <p>The Charging Station sends it further to the EV.</p> <p>The EV authenticates the signature of the bundle.</p> <p>Optionally: the EV checks the signature of the contract certificate.</p> <p>The EV decrypts the private key associated to the contract.</p> <p>The EV stores the private key securely in the EV.</p> <p>The EV or OEM (App) notifies the EV-User about the successful installation of the Contract Certificate.</p>
<b>Precondition/ Requirements</b>	Store the Signed Contract Certificate Bundle in the CCP.

	<p>The EV supports Contract certificate installation over the Charging Station and the PnC service is activated.</p> <p>A valid ISO15118 communication with a Charging Station supporting Contract Certificate installation should be in progress.</p> <p>The Contract certificate installation service is proposed by the Charging Station and selected by the EV.</p>
<b>Postcondition</b>	<p>The Contract certificate and the private key have been authenticated and securely installed in the EV.</p>
<b>Suggested technical solution / req. to ensure interoperability</b>	<p>It is recommended that all Charging Stations shall support Contract certificate installation.</p>

#### 2.1.4. Provide certificate for PnC in private environment

The objective of this sub-process is the setup of an EV with the required certificate for initiating 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, i.e., to enable encrypted communication and the transmission of charging session messages. In order to save costs, charging should take place with the same communication protocol on both public and private infrastructure. In the private environment however, complexity can be minimized by eliminating the use of OCSP and short-lived certificates, which eliminates the need for the EVSE to be constantly online.

- The Certificate management in the private environment can be simplified as well, compared to the public environment.
- By being a private environment, it is assumed that the user does not need to be billed or authorized through automated and standard means. Authorization and billing are the responsibility of the owner of the private environment instead.
- The PKI delivering certificates for the EVSE does not need to comply with requirements for the V2G PKI.
- Certificates validity period may be longer than EVSE certificates in 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 an offline authorization against a local whitelist.

There are several preconditions that have to be met in order 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 installed 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 was unchanged compared to charging in public.

#### 2.1.4.1. Install the private operator Root CA certificate in the EV through the Charging Station

<b>Objective</b>	Install the private operator Root CA certificate in the EV through the Charging Station.
<b>Short description</b>	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 in TLS setup.
<b>Actors involved</b>	EV, Charging Station
<b>Sequence and interface/ Communication channel</b>	<p>The EV is set into a PE “pairing mode”</p> <p>The EV and EVSE aligns on setting up TLS</p> <p>The EVSE sends the whole private operator EVSE certificate chain to the EV, including the root certificate.</p> <p>The EV stores the root certificate.</p> <p>TLS will be established.</p> <p>EV and EVSE may offer/select “contract-based payment” (PnC) or EIM</p> <p>In case of “contract-based payment”,</p> <ul style="list-style-type: none"> <li>the EV provides a contract certificate to the EVSE.</li> <li>The EVSE may not validate the certificate (due to lack of online connection).</li> <li>The EVSE may authorize the EMAID against a local whitelist.</li> </ul> <p>In case of EIM,</p> <ul style="list-style-type: none"> <li>the EVSE user provides authentication mean</li> <li>EVSE authorizes against it</li> </ul>
<b>Precondition/ Requirements</b>	<p>EVSE is located in a private environment</p> <p>EVSE is setup with a private operator certificate chain</p>
<b>Postcondition</b>	The EV is authorized.
<b>Suggested technical solution</b>	As a recommendation, the pairing mode might be established by a push-button function at EV side.

/ req. to ensure interoperability	
-----------------------------------	--

## 2.2. Use PnC contract certificate

This section describes how the certificates are used during charge once the initial setup of all parties is done as described in previous chapters.

These use cases are initiated automatically when an EV-User plugs in its ISO15118-compliant vehicle to an ISO15118-compliant EVSE (charging station). No user input or interaction should be required at this point, even if each OEM might add different ways for the EV-User to know if charging is in progress.

Main actors involved are:

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

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

- 2.2.1 Use of the Plug & Charge Contract certificate for authorization during a charging session
  - 2.2.1.1 Setup a TLS session to enable the Plug & Charge service
  - 2.2.1.2 Authenticate the Contract certificate to use for authorization
  - 2.2.1.3 Authorize charge using the Plug & Charge Contract Identifier (EMAID)

To assure a nominal charging process, several preconditions need to be fulfilled.

1. The use of the certificates at EV side requires such certificates to have been generated and/or installed on the EV.
  - Root CA certificates (OEM, V2G and if necessary eMSP) need to be set up and published.
  - Especially V2G RootCA certificates are required to be installed as trust certificates in the EV.
  - EV provisioning certificate needs to have been installed following 1.1.2 Provision OEM Certificates
2. A contract with an eMSP must have been signed and activated for this specific EV resulting in the generation of a contract certificate and associated Contract Certificate Bundle, which in turn must have been signed by a CPS and published.





3. The EV-User must have activated PnC feature and chosen the use of ISO15118 authentication means. Choice of other authentication means might be available but the charge in these alternatives does not require the following use cases.

As a result, and postcondition the vehicle is starting to charge. Revoked certificates are removed from certificate pools once the EV system is notified. The OEM is responsible of the removal of revoked contract certificates from the EV when needed.

### 2.2.1. Use of the Plug & Charge contract certificate for authorization during a charging session

<b>Objective</b>	To enable that the EV-User and its EV can be authenticated at the charging station using Plug & Charge based on ISO15118.
<b>Short description</b>	The EV-User plugs the charging cable into the EV and/or EVSE. As the charging cable is plugged in, the EV will automatically identify itself to the charging station, get authenticated and get authorization to receive energy for charging its EV battery.
<b>Actors involved</b>	EV, EV-User, EVSE, CSMS, CCP/CPS provider, PKI, OCSP responder, eMSP backend
<b>Sequence and interface/ Communication channel</b>	<p>This is an overall use case covering all functions of the use of certificates during the charging session.</p> <p>That session starts with plugging in the EV to an EVSE and should not require additional user interaction.</p> <p>The sequence then follows the next steps:</p> <ul style="list-style-type: none"> <li>– 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;</li> <li>– Optionally: Installation of a Contract certificate from a CCP through the EVSE;</li> <li>– Verification of the Contract certificate using a challenge sent by the EVSE (req. 899 from ISO15118-2) from the Charging station (ISO15118-2 PaymentDetailsReq/Res);</li> <li>– Authorization by the eMSP for payment based on the Contract certificate EMAID.</li> <li>– Start of power delivery during which no further interactions concerning certificates are in progress.</li> </ul> <p>This process mainly consists of 3 parts:</p> <ol style="list-style-type: none"> <li>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;</li> <li>2) Validation of the Contract certificate: This step could be managed by the respective CSO;</li> </ol>

	<p>3) Authorization process based on the EMAID: This step is managed by the eMSP and CSO (synchronously with a “realtime request”, or asynchronously based on a “whitelist”).</p>
<p><b>Precondition/ Requirements</b></p>	<p>Preconditions are described in chapter 1 and are referenced here.</p> <p>The following PKI use cases must be set up prior to the charging session.</p> <ul style="list-style-type: none"> <li>– UC 1.1.1.1 Register and Provide Root CA certificates for the PnC service</li> <li>– UC 1.1.2.1 Provide OEM Provisioning Certificate</li> <li>– UC 1.1.3.1 Install relevant certificates in the EVSE to enable the PnC service</li> <li>– UC 1.1.3.3 Install relevant certificates in the EVSE and CSMS to enable TLS for EVSE-CSMS communication</li> <li>– UC 1.2.5 Store the signed Contract Certificate Bundle in the CCP</li> </ul> <p>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.</p> <p>Other prerequisites: There is a roaming agreement between the eMSP and the Charge Point Operator.</p>
<p><b>Postcondition</b></p>	<p>The EV-User has successfully started the charging transaction using Plug &amp; Charge based on ISO15118.</p> <p>“Charging operation begins (has to be visible to the EV-User through the use of lights or display)</p> <p>Or an indication of an error is sent back and displayed to the user. On board display means are the responsibility of the OEM. The charging Station could display the status of the session to the user</p> <p>Error indication may also be shown by the charging station but not required.”</p>
<p><b>Suggested technical solution / req. to ensure interoperability</b></p>	<p>“Charging Station certificate authentication validation:</p> <p>Charging station must present its full chain up to but excluding a root recognized by the vehicle.</p> <ul style="list-style-type: none"> <li>– either containing multiple Cross Certification: certification path shall not exceed 4 levels</li> <li>– or with Trust List: EV should handle up to 5 V2G Root certificates, as recommended in ISO15118-2 specification.</li> </ul> <p>Verification of revocation is required (using OCSP Stapling)</p>

---

Authorization:

Challenge authentication for the contract certificate is required by V2G2-901 from ISO15118-2.

Contract Certificate authentication:

The CSO should check the full chain, even if the contract certificate does not contain the full chain. ISO15118-2 requests the EV to send the contract certificate full chain. The CSO has to ensure that this verification is done anyway, but it is recommended that the verification comes as early as possible to terminate invalid authorization requests at the earliest.

- Verification by the charging station requires that all SubCA are present on the charging station.

The charging station contacts then the CSMS.

The CSMS should be able to require an authorization for the right contract information based on EMAID.

The CSMS requests the eMSP for authorization”

---

### 2.2.1.1. Setup a TLS session to enable the Plug & Charge service

Objective	Authenticate the EV and the EVSE and establish a secure communication channel
Short description	<p>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.</p> <p>For -20 : In case the EV is set up for it, the EVSE will authenticate the EV as well.</p>
Actors involved	EV, EVSE, OEM OCSP Responder (For -20 only)
Sequence and interface/ Communication channel	<p>When plugged in, the EV initiates the connection to the EVSE following the TLS protocol:</p> <ul style="list-style-type: none"> <li>- TLS 1.2 (or later versions) protocol is to be used.</li> <li>- The EV asks the EVSE to establish a secure communication, sharing its supported Root CAs.</li> <li>- The EVSE responds with its SECC leaf certificate, its certificate chain and its Sub-CA certificates' OCSP status.</li> </ul> <p>The EV validates the certificate by checking the whole certificate chain and the OCSP status</p> <ul style="list-style-type: none"> <li>- EV and EVSE negotiate for the cipherSuite that they will use. Both EV and EVSE shall support cipherSuites specified in ISO15118-2.</li> </ul> <p>Both EV and EVSE generate the same master key and derived keys to encrypt and authenticate records.</p>
Precondition/ Requirements	<p>The V2G Root Certificate is installed in the EV</p> <p>The EVSE has been setup for ISO15118 authentication</p> <ul style="list-style-type: none"> <li>- It has obtained a SECC certificate and own the matching private key. That key must be securely stored.</li> <li>- It contains the certification chain of its own SECC certificates, up to the matching Root CA.</li> </ul>

	<p>The EVSE has obtained a valid OCSP status response for each of its CSO Sub CA certificates.</p>
<p>Postcondition</p>	<p>Transport &amp; security layers are ready for PnC charging operations.</p> <p>An indicator should show that charging session is in progress.</p> <p>In case of an error, an indicator should show that the charging session could not start.</p> <p>Additional detailed information might be available to the EV-User at the EV OEM and CPO discretion.</p>

<p>Suggested technical solution / req. to ensure interoperability</p>	<p>Use-case on Trusted List of Root-CAs vs. Cross-Certification.</p> <p>To ensure interoperability, ISO15118-2 requests the EV to handle a trust list of up to 5 V2G Root certificates.</p> <p>Cross certification may be more complex. The trust list seems a better solution, but is still under discussion at the ecosystem level.</p>
<p>Remarks</p>	<p>Charging Station certificate authentication validation:</p> <p>Charging station should present its full chain up to but excluding a root recognized by the vehicle.</p> <ul style="list-style-type: none"> <li>- either containing Cross Certification or</li> <li>- with Trust List</li> </ul> <p>Verification of revocation status is required (using OCSP)</p>

### 2.2.1.2. Authenticate the contract certificate to use for authorization

Objective	The EV authenticates using its contract certificate to confirm the possession of a valid certificate and associated private key.
Short description	<p>The EV requests for the ISO15118 authorization challenge. It presents its chosen contract certificate as well as the EMAID and the response to a challenge to ensure proof of possession of the private key.</p> <p>The charging station verifies the certificate validity and the challenge response</p>
Actors involved	EV, EVSE, OCSP Responder
Sequence and interface/ Communication channel	<ol style="list-style-type: none"> <li>1. The EV first presents the contract certificate and Sub-CA chain (with the PaymentDetailsRequest).</li> <li>2. The EVSE sends the (PaymentDetailsRes with the) challenge</li> <li>3. The EV sends the (AuthorizationRequest containing that) same challenge, signed with the private key that corresponds to the contract certificate</li> <li>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</li> </ol> <p>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.</p> <p>It is recommended that the contract certificate checks are processed at the earliest, so on the EVSE, whenever possible.</p> <p>It is recommended that a revocation check is also operated during certification validation. In the case of an offline charging station however, this revocation check may not be possible. Decision of implementing the revocation check is left to the CSO who will also be responsible for the wrong use of a certificate.</p>
Precondition/ Requirements	<p>The contract certificate is installed in the car</p> <p>The secure communication between the EV and EVSE has been established.</p>



	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.

### 2.2.1.3. Authorize charge using PnC Contract Id (EMAID)

Objective	Obtain the authorization for payment as prerequisite to the start of the energy charging, when the charging station is online.
Short description	After a secure communication between the EV and EVSE has been established and the contract certificate has been verified, the EVSE or CSMS obtain the authorization to start the charge.
Actors involved	EVSE, CSMS
Sequence and interface/ Communication channel	<p>The EVSE requests authorization from the CSMS based on the contract certificate and EMAID.</p> <p>The CSMS requests payment authorization from the eMSP</p> <p>The CSMS validates authorization and notifies the charging station to initiate the charge.</p>
Precondition/ Requirements	<p>The contract certificate is installed in the car</p> <p>The contract certificate is valid</p> <p>The EMAID has been obtained from the EV / Contract Certificate</p> <p>The CSMS has a means to secure communications with the eMSP</p>
Postcondition	<p>Authorization has been granted and transmitted to the charging station</p> <p>Charge begins</p>
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 ISO15118 PKI uses. There 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 usage.

## 2.3. Crypto-agility

Crypto-agility is a safety measure or incident response that intends to design information security protocols and standards in a way so that they can support multiple cryptographic primitives and algorithms at the same time. Its primary goal is to enable rapid adaptations of new cryptographic primitives and algorithms without making disruptive changes to the systems' infrastructure. In this document a small set of recommended practices are shared in order to help hardware manufacturers to implement crypto agility already even though it is not yet required.

### 2.3.1. Crypto-agility applied to PnC

In the ISO15118-2 standard there is no mention on crypto-agility support. Then, a system may be declared as conform to ISO15118-2 requirements even if it does not support any built-in crypto-agility concept. Nevertheless, it is a strongly recommended practice 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, extended key length has to be well prepared. Since it will lead to incompatibilities if only one system supports its algorithms and other systems don't support the new algorithms, changes have always to be implemented backward compatible.

Three options to update V2G entities Crypto Suite / new algorithm:

- 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)

### 2.3.2. Recommended practices

Design recommendations

- Define handling of "legacy" data after update (revocation and re-signing or valid until expiry, handling of legacy devices)
- Check IT system designs (backend) to support crypto agility (e.g.: no fix length for data structs, that include crypto) -reviewed, recommended
- Define allowed overlap / Transition handling for backwards compatibility during algorithms change phase
- In case of critical incidents / exploits it is recommended that an online update mechanism is in place as the cypher suite needs to be updated periodically to assure the security
- Ensure continuous evaluation of security level of available algorithms

#### Technical implementation recommendations

- Enable Cipher Suites (SW libraries / HW implementations of cryptographic algorithms) and credentials (cryptographic keys, certificates), to be updated during the lifetime of the a V2G entity, either to address incidents / exploits in existing libraries or to roll out new cryptographic algorithms.
  - o The Cipher Suite is a security relevant component, therefore the update has to be secured against manipulation. Trust anchors has to be available in the system, with backward compatibility, for a defined time slot to insure 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

Technical realization of cipher suite updates for a specific entity (EV, Backend System, CA, ...) are under the responsibility of the actor providing the V2G entity.

## 2.4. Implementation recommendations for specific actors

This chapter summarizes the recommendations to the OEM and eMSP regarding use cases where the actual sequence and implementation are left at their respective discretion. If these recommendations are taken into commonly and early in the process, it will help stakeholders in the Plug & Charge ecosystem to set up a robust and well-running system, with the aim of providing the best possible user experience.

Below are the functionalities concerned by these recommendations:

### 2.4.1 OEM specific recommendations

- 2.4.1.1 Activate or deactivate the Plug & Charge feature from the electric vehicle
- 2.4.1.2 Activate or deactivate the Contract certificate installation request from the electric vehicle
- 2.4.1.3 Managing Contract certificates from the electric vehicle
- 2.4.1.4 Ensure the PCID is used by authorized persons from the OEM perspective

### 2.4.2 eMSP specific recommendations

- 2.4.2.1 Ensure the PCID is used by authorized persons from the eMSP perspective
- 2.4.2.2 Unsubscribe from the e-mobility service of an eMSP
- 2.4.2.3 Terminate an e-mobility contract

As a recommendation for EVSE, if the charging station detects an EIM before starting the payment method sequence from ISO15118-2, the charging station shall use the EIM and refuse the Plug & Charge authentication mean.

### 2.4.1. 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 the systems in order to promote the adoption of electric vehicles by improving the user experience.

#### 2.4.1.1. Activate or deactivate the Plug & Charge feature from the electric vehicle

<b>Objective</b>	Allow the EV-User to choose his means of identification and payment for each of the charging sessions individually (e.g. e-mobility contract subscribed to an eMSP: RFID or Contract certificate, credit card, cash, ...). The solution must allow the Plug & Charge function of the EV to be deactivated and reactivated.
<b>Short description</b>	The EV-User activates or deactivates the Plug & Charge feature of his vehicle (e.g.: from the HMI of the vehicle or from the OEM application), allowing other users of the vehicle to identify themselves and pay by the means of their choice for benefit from the charging service.
<b>Actors involved</b>	EV-User, EV
<b>Sequence and interface/ Communication channel</b>	<p>1) The EV-User navigates in its user settings from the HMI of the electric vehicle or from the OEM mobile application and selects his means of identification.</p> <p>2) The EVCC uses the last user setting selected by the user for the next charging session.</p>
<b>Precondition/ Requirements</b>	<p>The OEM offers the possibility for the EV-User of adjusting its user settings relating to the means of identification:</p> <ul style="list-style-type: none"> <li>- The electric vehicle has all necessary prerequisites for the use of the Plug &amp; Charge feature;</li> <li>- The use of the Plug &amp; Charge feature can be easily deactivated temporarily until reactivation by the EV-User;</li> <li>- The EV-User has access to an interface: (e.g.: HMI of the electric vehicle or OEM application), to perform this operation.</li> </ul> <p>The user preference has to be set before plugging in the electric vehicle to the charging station.</p>
<b>Postcondition</b>	<p>While the Plug &amp; Charge feature is deactivated by the EV-User, the EVCC shall use the EIM for identification to the charging station.</p> <p>While the Plug &amp; Charge feature is activated by the EV-User, the EVCC shall request the Plug &amp; Charge identification with Contract certificate to the charging station.</p>
<b>Suggested technical solution / req. to</b>	User preference to be defined in the user settings from the HMI of the electric vehicle or from the OEM application.

<p><b>ensure interoperability</b></p>	
<p><b>Remarks</b></p>	<p>This choice is left to the user at any point before beginning charging.          The activation / deactivation process shall not exceed few seconds.          No change can be taken into account by the electric vehicle after plug in.</p>

#### 2.4.1.2. Activate or deactivate the Contract certificate installation request from the electric vehicle

<b>Objective</b>	The EV-User can activate or deactivate the installation request for specific Contract certificates by the charging station from its user interface.
<b>Short description</b>	The Plug & Charge feature allows the installation of Contract certificates by the OEM back-end or by the charging station. When the user wants to install a specific contract, he can request installation by the charging station. In this case, the vehicle must send the “CertificateInstallationReq” request according to ISO15118-2 specification, for the charging station to retrieve the available Contract certificate from a secondary actor, like a CCP. The EV-User has to activate the installation mode in the electric vehicle to send this message.
<b>Actors involved</b>	EV-User, EV (OEM)
<b>Sequence and interface/ Communication channel</b>	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 the communication with the charging station, the electric vehicle sends the “CertificateInstallationReq” message to request installation of the Contract certificate.
<b>Precondition/ Requirements</b>	The Plug & Charge feature is activated in the electric vehicle.
<b>Postcondition</b>	The electric vehicle is enabled to install a new contract certificate through the charging station.
<b>Suggested technical solution / req. to ensure interoperability</b>	None, the implementation is OEM specific.



### 2.4.1.3. Managing Contract certificate from the electric vehicle

<b>Objective</b>	The EV-User can manage his Contract certificates from his OEM application, or from the vehicle interface (installation and uninstallation from the vehicle). He can easily select the Contract certificate to activate to access the next upcoming charging service, independently of the eMSP.
<b>Short description</b>	<p>The EV-User has subscribed to one or more e-mobility contracts.</p> <p>In his personal settings (from the OEM application or from the electric vehicle), the user selects a default contract. The related Contract certificate and related private key must be installed in the electric vehicle to be presented to the station during the upcoming charging session.</p> <p>The user may request the installation or uninstallation of other e-mobility contracts from the OEM application or from the electric vehicle. Consequently, the user must be able to change its default contract easily, for example for price differences, or for the use of company or rental vehicles.</p>
<b>Actors involved</b>	EV-User, EV, OEM
<b>Sequence and interface/ Communication channel</b>	<p><b>Sequence needs to be defined by the OEM, following statements are requirements:</b></p> <p>The EV-User should be able to get a list of all the Contract Certificates installed in the EV that he is authorized to use.</p> <p>The EV-User should be able to select one Contract Certificate for which he is authorized to use as default for next charging sessions.</p> <p>The EV should provide information to the EV-User of the Contract Certificate used for next charging session.</p> <p>For installation of a new contract certificate, the EV should ensure that the EV-User is authorized to install this certificate.</p> <p>The EV-User should be able to choose to be notified of any changes on his contract certificates installed.</p>
<b>Precondition/ Requirements</b>	<ul style="list-style-type: none"> <li>- The EV-User has subscribed to one or more e-mobility contracts.</li> <li>- The EV-User has a digital interface (e.g.: HMI in the EV or OEM application) allowing him to interact with the electric vehicle settings, in particular switching between e-mobility contracts.</li> </ul>

	<ul style="list-style-type: none"> <li>- The default configuration (activated Contract certificate) is defined before the electric vehicle is plugged in.</li> <li>- UC 1.2.3 is executed.</li> <li>- The EV-User has not selected any Contract certificate for the charging process or would like to change the selection he has already made.</li> </ul>
<b>Postcondition</b>	<ul style="list-style-type: none"> <li>- One or more e-mobility contracts are installed in the electric vehicle.</li> <li>- Only one e-mobility contract is set by default by the EV-User.</li> <li>- The EV-User gets user-friendly information about which e-mobility contract is active on his digital interface.</li> <li>- The EV-User selection is encrypted to be stored securely in his/her personal settings, and is available in the electric vehicle.</li> <li>- The electric vehicle used the Contract certificate activated by the EV-User (default).</li> </ul> <p><u>Optional:</u></p> <ul style="list-style-type: none"> <li>- The EV-User may authorize other EV-Users to use its Contract certificate selection.</li> </ul>
<b>Suggested technical solution / req. to ensure interoperability</b>	<ul style="list-style-type: none"> <li>- Comply with VDE-AR-E 2801-100-1 §11.2.4</li> <li>- The OEM may implement EV-User profiles.</li> <li>- The switching process should only take a few seconds.</li> <li>- The configuration is carried out before the vehicle is plugged in to the charging station.</li> <li>- 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.</li> <li>- A user-friendly OEM application and electric vehicle interface should be implemented.</li> </ul>
<b>Remarks</b>	<p>The EV-User should be able to get a list of all the Contract Certificates available in the CCP that he is authorized to use.</p>

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

<b>Objective</b>	Prevent the misuse of the Plug & Charge Contract certificates, especially for car sharing, rental and fleets.
<b>Short description</b>	<p><b>General remark:</b> The PCID is non-confidential data, shared through the PKI of the Plug &amp; Charge ecosystem. The customer of a mobility contract taken out with an eMSP is responsible for linking the correct PCID to his contract. The OEM is responsible for installing only authorized Contract certificates.</p> <p>The OEM has the interest to defend the misuse of the PCID (e.g.: for the installation of the Contract certificate in the electric vehicle without permission of EV-User). This use case is specific to the OEM implementation.</p>
<b>Actors involved</b>	eMSP, eMSP customer, OEM, EV, PCP
<b>Sequence and interface/ Communication channel</b>	-
<b>Precondition/ Requirements</b>	-
<b>Postcondition</b>	-
<b>Suggested technical solution / req. to ensure interoperability</b>	<p>Only approved Contract certificates should be installed in the electric vehicle, i.e. the ones authorized by the EV-Owner or delegates.</p> <p><u>Potential measures:</u></p> <ol style="list-style-type: none"> <li>1) The OEM blocks the installation of unauthorized Contract certificates in the electric vehicle.</li> <li>2) The OEM provides means to transmit the PCID directly to the eMSP with permission of the EV-Owner (Authentication framework like Oauth2.0).</li> <li>3) The OEM provides the PCID only to authorized entities (e.g., through OEM application, with PIN authorization in the vehicle dashboard). The OEM provides security measures against disclosure of the PCID.</li> </ol>

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

## 2.4.2. eMSP specific recommendations

This section offers specific recommendations for managing the end of the mobility contract or the relationship with the eMSP, meeting user and security needs. Their implementation falls within the technical choices of the eMSP, but aim to propose good practices to ensure coordinated management of the ecosystem.

### 2.4.2.1. Ensure the PCID is used by authorized person from the eMSP perspective

<b>Objective</b>	Prevent the misuse of the Plug & Charge Contract certificates, especially for car sharing, rental and fleets.
<b>Short description</b>	<p><b>General remark:</b> The PCID is non-confidential data, shared through the PKI of the Plug &amp; Charge ecosystem. The customer of a mobility contract taken out with an eMSP is responsible for linking the correct PCID to his contract. The OEM is responsible for installing only authorized Contract certificates.</p> <p>The eMSP has the interest to ensure that the correct PCID is given 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.</p>
<b>Actors involved</b>	eMSP, eMSP customer, OEM, EV, PCP
<b>Sequence and interface/ Com. channel</b>	-
<b>Precondition/ Requirements</b>	-
<b>Postcondition</b>	-
<b>Suggested technical solution / req. to ensure interoperability</b>	<p>The eMSP ensures that the PCID is correctly submitted by the its client (eMSP customer, OEM).</p> <p><u>Potential measures:</u></p> <ol style="list-style-type: none"> <li>1) The eMSP provides means to obtain the PCID from the OEM directly with the permission of the EV-Owner (Authentication framework like OAuth2.0)</li> <li>2) The eMSP provides means to get the PCID from its client (e.g.: OCR, QR-code reader)</li> </ol>

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

#### 2.4.2.2. Unsubscribe PnC certificate for a given EV (PCID)

<b>Objective</b>	Contract certificate becomes invalidated either by customer for a certain PCID or by end of subscription.
<b>Short description</b>	eMSP customer informs eMSP to end validity of PnC service for certain electric vehicle (PCID). All PCID related contract certificates will be revoked and/or deleted.
<b>Actors involved</b>	eMSP customer, eMSP, OEM, EV, CAs (for CRL and OCSP service), CCP, CPS
<b>Sequence and interface/ Communication channel</b>	<ul style="list-style-type: none"> <li>• eMSP customer informs eMSP to disconnect EV from eMSP contract (and end validity of PnC service for certain electric vehicle (PCID)).</li> <li>• EMSP informs respective CAs hosting the CRL and OCSP services for contract certificates about revocation of contract certificate(s)</li> <li>• CAs revoke contract certificates</li> </ul>
<b>Precondition/ Requirements</b>	- EMSP has created valid contract certificate for certain PCID (which might be already signed by CPS, stored in CCP/at OEM/ in EV)
<b>Postcondition</b>	<ul style="list-style-type: none"> <li>- The electric vehicle is not able to charge using the contract certificate anymore.</li> <li>- CPS, CCP, OEM, EV delete respective certificates <ul style="list-style-type: none"> <li>○ The revocation status is sent to the electric vehicle by the charging station during the ISO15118 authorization process, OR</li> <li>○ The electric vehicle receives is notified by the OEM back-end that the Contract certificate is revoked.</li> </ul> </li> </ul>
<b>Suggested technical solution / req. to ensure interoperability</b>	CPS, CCP, OEM, EV should act immediately as soon as the revocation information was shared. They therefore should have a message system in place to be able to receive such data in real time.

### 2.4.2.3. Terminate an e-mobility contract

<b>Objective</b>	The e-mobility contract ends with the customer's action or at the end of subscription.
<b>Short description</b>	The customer ends the e-mobility contract. All related Contract certificates are revoked and/or deleted.
<b>Actors involved</b>	eMSP customer, eMSP, OEM, EV, CAs (for CRL and OCSP service), CCP, CPS
<b>Sequence and interface/ Communication channel</b>	<p>1) Request for termination of the Plug &amp; Charge service:</p> <ul style="list-style-type: none"> <li>- The eMSP customer requests the eMSP to terminate the contractual relationship OR</li> <li>- Once the subscription termination date is reach, the eMSP SubCA adds the Contract certificate associated with the vehicle to its revocation list.</li> </ul> <p>2) The eMSP informs the eMSP customer that Plug &amp; Charge service will be ended for all associated vehicle(s) connected to that eMSP relationship.</p> <p>3) Use Case 4.2.2 applies</p> <p>5) The electric vehicle deletes the Contract certificate.</p>
<b>Precondition/ Requirements</b>	<ul style="list-style-type: none"> <li>- The eMSP customer has valid contractual relationship with the eMSP.</li> <li>- The Contract certificate is still be valid, OR</li> <li>- The Contract certificate is already revoked and deleted.</li> </ul>
<b>Postcondition</b>	<ul style="list-style-type: none"> <li>- The Contract certificates are revoked, and the revocation information has been distributed (e.g.: CRL/OCSP).</li> <li>- The Contract certificates are removed from the electric vehicle and from all back-ends (CCP, CPS, OEM, eMSP).</li> </ul>
<b>Suggested technical solution / req. to ensure interoperability</b>	The OEM back-end is notified when EV specific Contract certificates are revoked and removed automatically.



### 3. Conclusion & Next Steps

This guide should serve as a base for future developments in order to assure interoperability in the future. We do recognize that it will not represent the full scope of all activities on the market but should cover the majority of all use cases. Should there be additional use cases that have not been addressed and are found missing please inform CharIN that those can be included in a next revision of the document.

#### 3.1. Future evolutions and scope considered for the document

The following items are not described in the present document and will be integrated in future releases:

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

## 4. Reference

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

Contributing Authors:

Ronald Heddergott (CARIAD)

Jean-Marc Rieves (Gireve)

Michel Girier (Gireve)

Steffen Rhinow (Hsubject)

Alexander Plath (Shell)

Marc Mültin (Switch)

Mourad Tiguercha (Vedecom)

Nicolas Lheraud (Vedecom)