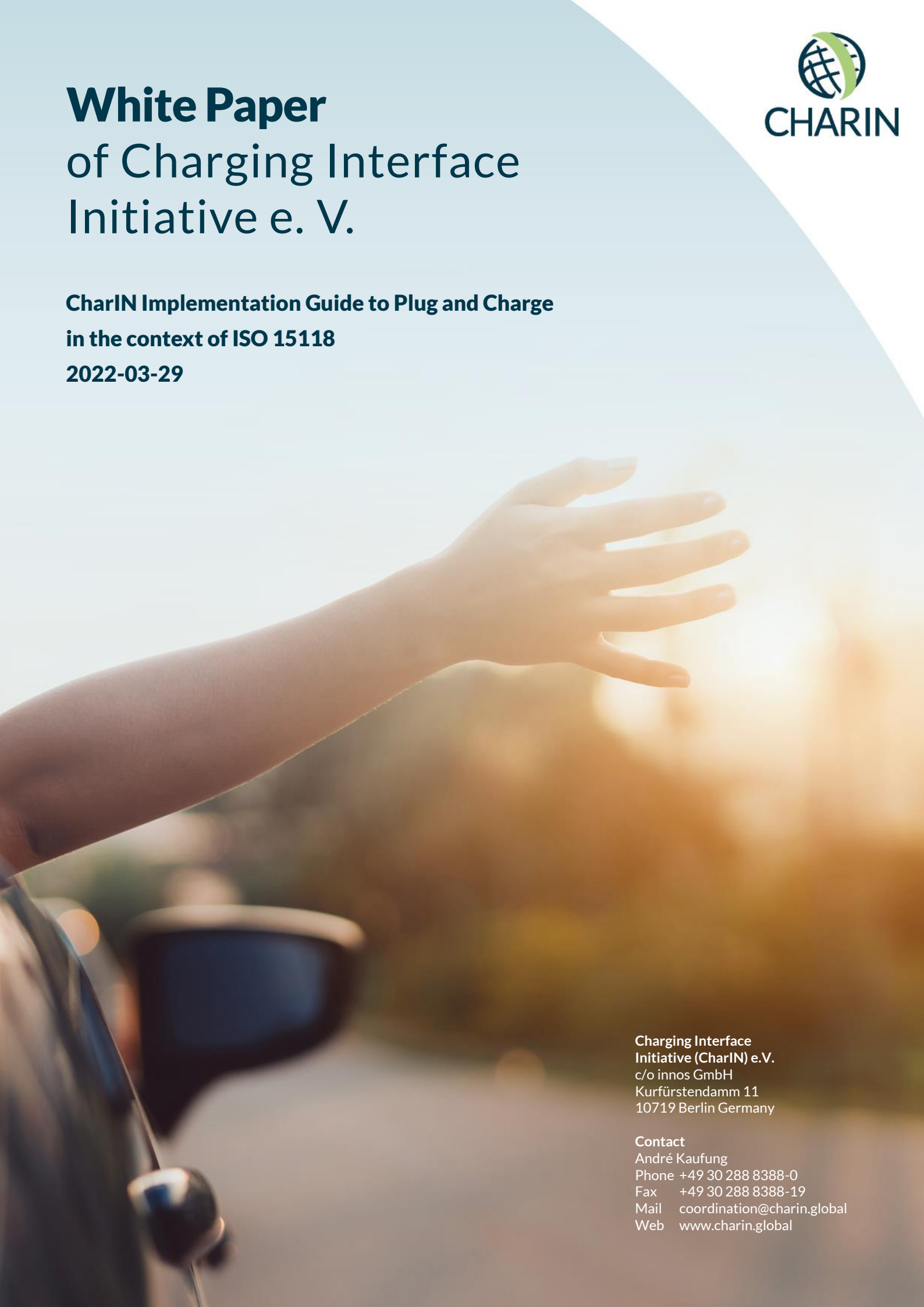
White Paper
of Charging Interface Initiative e. V.

CharIN Implementation Guide to Plug and Charge in the context of ISO 15118
2022-03-29



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
Web www.charin.global

Contents

1. Preface

This document has been written on behalf of Hubject GmbH, CharIN e. V. and with input from other industry participants. The authors would like to express their gratitude to the other contributors.

2. Management Summary

This implementation guide is meant for implementers on OEM side and aims at achieving four major goals:

- Provide a brief introduction to the e-Mobility market, its actors and their relation to ISO 15118 – 2:2014
- Introduce the major concepts and used technologies of ISO 15118 – 2:2014
- Ease the implementation of Plug&Charge in compliance with ISO 15118 – 2:2014 for all EV market participants with a more practical approach, by elaborating on the most crucial use cases
- List the most prevailing implementation related requirements for both the ISO 15118 – 2:2014 protocol stack and the needed certificate exchanges

3. Introduction

3.1. About CharIN e.V.

The Charging Interface Initiative e. V. (CharIN e. V.) is a registered association with members along the whole value chain of EV charging and is open to all interested parties.

The target of the initiative is to continuously and competently implement the Combined Charging System (CCS) and the Megawatt Charging System (MCS) with the objective of establishing these systems in the global market.

Mission of CharIN e. V.:[1]
Expanding the global network by integrating companies on each level of the defined value chain to support and promote CCS and MCS

Drafting requirements to accelerate the evolution of charging related standards

Defining a certification system for all manufacturers implementing CCS and/or MCS in their products

3.2. Background of the ISO 15118 standard

Two previously independent sectors are now connected by the electric vehicle: the automotive and the energy supply industry. The synergy potential of this cooperation also depends on standardized interfaces between EVs and the electricity grid. ISO, the International Organization for Standardization, has defined the interfaces for customer-friendly and interoperable charging (Plug&Charge) as well as the integration of electric vehicles into the energy network (Smart Charging) in the international ISO standard 15118. Thus, the technical framework for different variations of integrating electric vehicles in intelligent power networks has been developed and a signal of investment safety has been created for automotive manufacturers and energy suppliers.

Digital certificates play an important role in this machine-to-machine communication – and in the EV network too. Plug&Charge technology allows automated communication between electric vehicles and charging stations. The requirements of this communication are defined in ISO 15118 – 2:2014. The overall aim of this international standard is to charge electric cars without requiring the driver to interact with the charging station.

Secure authentication and authorization are essential for this technology. Therefore, digital certificates in accordance with ISO 15118 – 2:2014 are used to secure communication between EVs and charging stations. Certificates are data blocks which are electronically signed by a trusted Certificate Authority. The technology used in this process is called Public Key Infrastructure (PKI) and is based on asymmetric encryption. [2][3]

[1] www.charin.global
[2] Christian Hahn, Sebastian T. Crusius – EVS30 symposium 2018
[3] VDE-AR-E 2802-100-1 https://www.dke.de/de/normen-standards/dokument?id=7095892&type=dke%7Cdokument

3.3. Secure Communication

Within the ISO initiative scope a modern IT communication process between EVs and charging station was developed. The process takes into account existing standards and supplements safety-relevant components. Based on certificates, the ISO standard 15118 regulates the automated and secure data exchange between EVs and the charging infrastructure. It also describes general applications and information flows of charging and payment processes. Technologies such as inductive and bi-directional charging, which are still under development, are also integrated into the standard. Without further interaction with the charging station on the part of the driver, charging of EVs will become even more straightforward, which is the overall goal. This requires the EV and the charging station to be securely authenticated and authorized. At the same time, all processes between the EV and the charging station have to be carried out automatically and safely – EV drivers only have to connect the charging cable in the Plug&Charge use case.

3.4. Business Models of ISO 15118

The ISO standard 15118 laid the foundation for communication between EVs and charging infrastructure. However, many processes are not yet sufficiently defined as other players, like electric grid operators, fleet managers, electric utilities and third-party providers, are involved in the value chain of charging processes and value-added services. There are already numerous reasons for all relevant players in the e-Mobility market to include the new ISO standard in their own business models.

Another reason to implement this charging standard at an early stage is the financial support of charging systems that acknowledge this standard, which includes initiatives from various national governments. For example, the German government has already made the ISO standard 15118 an integral part of the planned subsidy program for public normal and fast-charging infrastructure, which totals € 300 million, in order to build charging stations, which are equipped for the future. Likewise, the US state of California has specified that the implementation of the standard is clearly in line with the ISO 15118 – 2:2014 requirements and should be applied to all charging stations.4

Through these and other market developments it is to be assumed that the integration of the charging standard will be relevant for each of the following company types in the short and long run.

The charge point operator (CPO) is a classic charging process stakeholder and, as an operator of the charging station, is particularly committed to implementing ISO 15118. Energy suppliers and public services occupy this role. In order to automatically communicate with the electric vehicle through the charging station, the

[4] http://www.cpuc.ca.gov/WorkArea/DownloadAsset.aspx?id=6442455245

latter must be able to process the information of the vehicle and "identify" itself. The charging station acts as a server and responds to the electric car's messages. Corresponding requirements are not only the responsibility of the charging station hardware, but also the back-end software.

The Mobility operator (MO) is defined to play an important role in the charging process in accordance to ISO 15118. On the one hand, the MO sells the driver or owner of an EV a contract, on the other hand, it is responsible for the authentication method and for issuing the contract certificate.

The original equipment manufacturer (OEM) produces the ISO 15118 compatible EVs and publishes the OEM provisioning certificates for the MOs. By means of an OEM provisioning certificate (installed in the vehicle), the OEM has to make sure that the electric vehicle is already prepared for all possible circumstances within the certificate administration upon delivery.

The offering of value-added service by means of an extended relationship with customers over the service cycle of the EV has significantly driven the auto OEMs to support the implementation of ISO 15118.

For the EV drivers, ISO 15118 Plug&Charge offers a great customer charging experience. Other important advantages incorporated in the new standard include: automatic authentication and authorization at all charging points via e-Roaming technology, high security against data manipulation through integrated information security, and the optimization of charging processes based on energy demand and departure time.

At the same time, the implementation of the standard makes it possible for MOs and CPOs to forecast the energy demand and optimize grid utilization, to integrate renewable energies into electricity offers and to provide time-variable tariffs as well as to use non-moving vehicles for temporary storage. In addition, the simplification of activating the charging station is possible by eliminating RFID cards through certificate-based communication (EV to EVSE) and the offering of value-added services such as charge spot reservation or required energy for next usage of the EV.

3.5. Future Proof Charging Infrastructure

The basic conditions of ISO 15118 which have a significant impact on the development of a viable charging infrastructure and the establishment of new business models are still being clarified. Nevertheless, each of the market players described is advised to consider the subject of charging infrastructure for electric vehicles as part of current considerations. Be it in the bidding for new charging stations or in the development of new electric power or customer products. ISO 15118 demonstrates that e-Mobility is based on cooperation between stakeholders from the energy, automotive, and IT industry. The establishment of relevant collaborations and partnerships helps to develop new business areas and to shape the technological development of e-Mobility at an early stage.

3.6. Goals of this Document

This implementation guide is meant for implementers on all EV business models and aims at achieving four major goals:

- Provide a brief introduction to the e-Mobility market, its actors and the relation to ISO 15118
- Introduce the major concepts and used technologies of ISO 15118
- Ease the implementation of Plug&Charge in compliance to ISO 15118 – 2:2014 for all EV market participants with a more practical approach, by elaborating on the most crucial use cases
- List the most prevailing implementation related requirements for both the ISO 15118 – 2:2014 protocol stack and the needed certificate exchanges

4. EV ecosystem

4.1. Market roles and responsibilities

4.1.1. V2G Root Operator (V2G Root)

The V2G Root operator is responsible for the management of the V2G root CA, which is the highest trust anchor in ISO 15118 – 2:2014. It securely creates a V2G root certificate and provides for all the stakeholders of ISO 15118. It may also be the responsibility of the V2G Root operator to provide certificates for the electric vehicle supplier equipment (EVSE) and signing the contracts of the mobility operators to ensure the validity and security.

4.1.2. Charge Point Operator (CPO)

Includes companies, which are responsible for the management and servicing of the charging device and charging stations. Its main responsibilities concern the management of the charging points by means of an IT system, the billing and invoicing, either directly to the driver or to a mobility operator.

4.1.3. Mobility Operator (MO)

Organizations that offer a wide range of charging related services to the end customer to search and find a charging station as well as to authenticate and pay for a charging session. The MO concludes a commercial contract with the EV owner or driver.

4.1.4. Original Equipment Manufacturer (OEM)

OEM stands for 'original equipment manufacturer' and, in the context of electric mobility, is always associated with vehicle manufacturers. OEMs shall enable end customers to conduct automated charging and billing processes.

4.2. Relevant associated protocols

- Other protocols which need to be considered are OCPP 1.6 / 2.0 for the communication between CPO backend and charging stations, Appendix I, for an alignment of messages. [5]
- Roaming protocol of OICP for processing charging session detail records and regular authorization data. [6]
- Other roaming protocols also co-exists, examples are OCPI and OCHP.

[5] http://openchargealliance.org/protocols/ocpp/ocpp-20/
[6] https://www.hubject.com/en/downloads/oicp/

There are currently globally two standardization bodies active in the development of standardized protocols between the charge point operator backend and their EVSEs. The working group TC 69 with the standard IEC 63110 will aim for a standardized protocol as well as the IEEE 2690 standard.

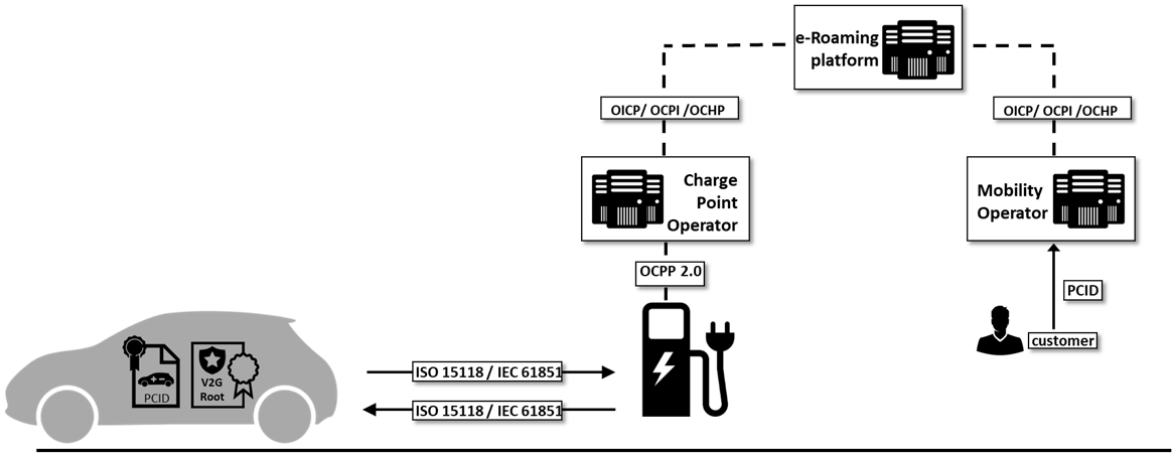


Figure 1 - Protocol overview

5. Communication protocol ISO 15118

5.1. Background

In 2009, both the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) together established an initiative for standardization of an IP-based communication protocol between an electric vehicle (EV) and charging stations (EVSE). The Vehicle-to-Grid Communication Interface (V2G CI) based on and complementing the international standard to IEC 61851-1 providing bi-directional digital communication. This new standard should enable Plug&Charge functionalities for seamless authentication, authorization, billing and load management, based on message exchanges between EVs and EVSEs. The messages included a contract of the MO, in such a way that external identification means were not needed anymore as the contract of the MO is stored in the EV and can be automatically recognized by the EVSE and vice versa.

5.2. Business opportunities with ISO 15118

The basic conditions of ISO 15118, which have a significant impact on the development of a viable charging infrastructure and the establishment of new business models, are still being clarified. Nevertheless, each of the market players described is advised to look into the subject of charging infrastructure for electric vehicles as part of current considerations. Be it in the bidding for new charging stations or in the development of new electric power or customer products.

5.2.1. First mover advantages

With this standard in the EV market being relatively new, and applicable to all participants, CPOs and MOs could gain first mover advantages by their ability to be better and more technology savvy than their competitors.

5.2.2. Value Added Service offering

With ISO 15118, value added services could be offered to maximize the convenience of end-customers, e.g. the ability to reserve a charge point, route information, smart charging services, etc. Additionally, the end-customer does not have to think about the hassle with (various) RFID cards anymore leading to an improved customer experience.

5.3. Secure communication

Secure TLS connection and the exchange of digital signed certificates ensure a secure exchange of (sensitive) customer-related information.

It is important to point out that if external identification means (EIM) are used such as RFID cards, remote authorization and others, channels to communicate these credentials should be secured separately.

Overall security of the system defined by the weakest link of this system such as the EIM communication channel not being secured at all or having lower level of security than ISO 15118 with TLS enabled, could put the whole information exchange process in higher risk.

Part 2 of the ISO 15118 v2.0 specification elaborates on the security aspects of the standard. The first characteristic of security, confidentiality, is assured by encrypting and decrypting messages via a TLS secured channel. Additionally, authenticity and integrity are supported by the application of hash algorithms and the generation and verification of digital, XML based signatures.

Confidentiality
The actual content of the message will only be readable by the intended recipient(s), but not by any unauthorized third parties.

Integrity
An unauthorized modification of the sent message shall be avoided or least be detected.

Authenticity
It shall be possible to assert that the communication actors are really the person or entity they claim to be. The genuineness of the transmitted message(s) must be ascertainable.

TLS connection establishment

Transport Layer Security (TLS) is a group of protocols that specify the establishment of an encrypted connection using a transport protocol (usually TCP). Previously, the name SSL - Secure Sockets Layer was used. However, version 3 of SSL corresponds to version 1 of TLS after renaming.

TLS is assigned to layer 5 in the OSI protocol stack and is based on X. 509 certificates in practice. In the past, attacks on older TLS and SSL versions have been known repeatedly, so at least v1.3 (IETF RFC 8446) should be used. The main differences between the different protocol versions are the supported cryptographic primitives (Cipher Suites). The validation of the certificates of communication partners is a central challenge for TLS, as it is the only way to authenticate them and thus prevent man-in-the-middle (MITM) attacks.

6. System Components in ISO 15118

This chapter describes the necessary components of the Plug&Charge Ecosystem and their purpose of use.

6.1. Root Certificate Pool – RCP

The Root Certificate Pool is used for the exchange of the root certificates between the various Certificate Authorities of ISO 15118 participants (V2G, OEM, MO). Each ISO 15118 participant can receive the root certificates of the other participants to validate the certificate chains.

6.2. Provisioning Certificate Pool – PCP

The Provisioning Certificate Pool (PCP) provides interfaces to exchange the OEM provisioning certificates between OEMs and MOs.

After the production of the EVs, the OEMs can publish the vehicle certificates (OEM provisioning certificates) of EVs in the PCP. The OEM provisioning certificates are used by the mobility operators to create contractData for the customers, which are uniquely calculated for each EV.

The MOs can access to the OEM provisioning certificates by sending the OEM provisioning certificate ID (PCID) of the vehicle certificate, which is issued by the OEM. The PCP delivers the appropriate OEM provisioning certificate and the corresponding sub-CA certificate chain.

6.3. Mobility Operator - MO

The mobility operators are the companies, which conclude e-mobility contracts with their customers. The customers deliver the unique PCID of the EV to the MO during the conclusion of a contract, which will be used by the MO to receive the OEM provisioning certificate from the PCP. In the first step, after the conclusion of the contract, the MO generates a unique e-mobility account identifier (EMAID) for this contract and generate a contract certificate and uses the EMAID as its common name.

In the second step, the MO creates a contract data, as defined in ISO 15118 – 2:2014. The created contract data must be signed by the certificate provisioning service (CPS) for the verification of authenticity and integrity in the EV.

6.4. Certificate Provisioning Service - CPS

The CPS provides interfaces for the signing process of the contract data. During the signing process, the CPS adds the provisioning certificate and the provisioning sub CA certificates into the contract data and creates a signed contract data (“certificateInstallationRes”), which is also defined in the ISO 15118 – 2:2014.

After the creation, the signed contract data must be stored in the Contract Certificate Pool (CCP) for provisioning to the CPO and OEM backends.

6.5. Contract Certificate Pool – CCP

The CCP is the main storage and publishing point of the signed contract data for the OEM and CPO backends.

The Application Rule describes two main possibilities for the provisioning of the signed contract data, via charging device (EVSE) or OEM backend.

After the successful TLS handshake between an EV and charging device, the EV creates a signed "certificateInstallationReq", which is defined in the ISO 15118 – 2:2014. This request will be forwarded by the CPO backend to the CCP and respond by the available signed contract data, as "certificateInstallationRes".

In case of using OEM backend, the CCP sends the signed contract data to the backend of the OEMs automatically without the delivery of a "certificateInstallationReq" from EV.

The third possibility is an offline certificate Installation[7]. A signed contract data may have to be transmitted to the vehicle without using the charge protocol. This may be necessary, if the infrastructure, the secondary actor or the vehicle does not support the certificateInstallationReq. In this case, the signed contract data is transmitted to the customer via postal or electronic mail, to install into the EV via e.g. using the diagnosis interface of the vehicle or an internet access to the vehicle.

6.6. PKI Services

Those companies playing an ISO 15118 market role that choose to create certificates in the ISO 15118 context, will need the following PKI infrastructure components:

- Certificate Manager Software: For the management of the certificates
- A Secure Storage: For generating and storing of the private keys securely
- Certificate Revocation List (CRL) distribution point: Publishing the revoked certificates as CRL
- Optionally OCSP responder[8]: Publishing the certificate status information

The relaying parties must also publish Certificate Policies and Certificate Practice Statements of their PKI services.

[7] ISO 15118 – 2:2014, Chapter 8.4.3.11.4 Offline Certificate Installation

[8] In ISO 15118 – 2:2014, operating an OCSP responder is optional.

7. ISO 15118 and VDE Application Guide

7.1. Introduction

The technical basis for the authentication with Plug&Charge is defined within the ISO 15118 – 2:2014 Edition 1. However, ISO 15118 – 2 Edition 1[9] lacks a full definition of secondary actors and required processes within the ecosystem of Plug&Charge. The ambiguities within the standard lead to situations where different implementations were considered as standard conform, therefore an additional document called the VDE Application Rule was written.

7.2. VDE Application Rule 2802

In order to provide a unique and industry wide implementation scenario, a working group (AK 901.0.115) within the "Deutsche Kommission Elektrotechnik Elektronik Informationstechnik" (DKE) was organized to draft a proposal for a full implementation of Plug&Charge ecosystem. As a result, an Application Rule for "Handling of certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO 15118"[10] was officially published in "October 2017" and will be an English version available in early 2019.

The VDE application guide applies to all actors involved in the context of DIN EN ISO 15118 (all parts). The objective of this VDE application rule is to define the currently unresolved gaps in specifications for the secure exchange of digital key materials and certificates between the actors involved and to put forward possible technical alternatives for the installation of a contract certificate in the vehicle and the necessary procedures for revoking a contract certificate. It also recommends actions that can be regarded as compliant with the standards of DIN EN ISO 15118 (all parts). [11]

An important requirement in ISO 15118-2 is that certificates need to be delivered within 5 seconds, using the message pair **CertificateInstallationReq/Res**. Hence, the VDE Application Rule covers the following topics:

- Role definitions and processes
- Data exchange between stakeholders
- PKI implementation topology using certificate pools
- Relation between the Contract ID and EMAID
- Revocation of contract certificates
- Accordance to ISO 27001 [12]

[9] Edition 2 of ISO 15118-2 is in draft form "Now under development" and estimated publication is 2019. The link to ISO/DIS 15118-2: https://www.iso.org/standard/69114.html. Previous document was ISO 15118-2:2014.
[10] VDE-AR-E 2802-100-1:2017-10
[11] https://www.iso.org/standard/55365.html
[12] https://www.iso.org/isoiec-27001-information-security.html

8. Certificate Management with ISO 15118

8.1. Conformity with RFC 5280 and X.509v3

As of today, EV drivers with an MO contract can authenticate themselves at the charging station via RFID card (UID) or smartphone app (EVCOID). In future, authentication via Plug&Charge will be achieved via distribution and validation of IT Certificates (X.509v3). In general, Root CA certificates, Sub-CA certificates should follow the certificate format specification in Annex F of ISO 15118-2 v2.0. These formats are conforming to RFC 5820, which on turn is based on X.509v3 format. The Certificate Manager should be fully compliant to RFC 5820 and X.509v3, and no special configuration is needed to assure this compliance. Default certificate formats are available for RFC 5820 compliant CA certificates.

8.2. PKI Infrastructure

The Public Key Infrastructure (PKI) is a common description of a cryptologic verification system for digital certificates. The PKI usually contains the following roles and responsibilities:

- **Certification Authority (CA)**: Responsible for the operation of the Root CA and signing of underlying Sub-CAs or certificates
- **Certificate:** A public key that is signed by a certificate authority. There are also self-signed certificates, which are the root certificates (e.g. V2G, MO and OEM roots)
- **Certificate chain:** Certificates can be signed in a kind of chain. For example, a trustworthy root instance (Root CA) signs a sub-instance (Sub-CA) and this sign the individual certificate (Leaf Certificate). Using the certificate chain, the individual certificate can be expanded down to the root instance and validated against it.
- **Certificate Signing Request (CSR):** A request to create a certificate from a public key using a signature.
- **Certificate Revocation List (CRL)**: A certificate list to publish the revoked and untrusted certificates for all certificate users. This list must be signed by the issuer CA to prove the authenticity.
- **OCSP Responder**: An online component to publish the certificate statuses, if it is “good”, “revoked” or “unknown”. Different than CRL, OCSP responder publishes the certificate status of one certificate in each request. The OCSP responders are defined optional in the ISO 15118 – 2:2014.
- **Directory Service**: Responsible for the provisioning of the OEM provisioning certificates and the signed contract data.

To ensure that a public key is trustworthy, it is signed by a trusted CA. In ISO 15118 – 2:2014 only asymmetric encryption is used. This means, two different keys must be generated, public and private key:

- **Pair of keys**: Combination of private and public key, generated in the same time as a pair.
- **Private key:** The secret key for signing and decrypting the data. This key must be secured very carefully. In case the private key is lost or published the public key will no longer be trusted and must be generated again immediately.
- **Public key:** The public key is used to encrypt data. This key cannot be used in any signing or decrypting operation. Public key is the signed part of the key pairs, which become a certificate.

- **Certificate**: The public key can be sent to a CA as a certificate signing request (See RFC2986). The CA signs this request and creates a certificate.

The following terms are used for the individual certificates according to ISO 15118:

- **Charging device certificate**: EVSE Leaf certificate with unique EVSE-ID
- **OEM provisioning certificate:** Vehicle certificate with unique provisioning certificate ID.
- **Provisioning certificate:** A certificate, which used to sign the contracts in the Certificate Provisioning Service.
- **Contract certificate:** Contract Leaf certificate with unique e-mobility account identifier (EMAID)

In the following chapters you can find detailed information about each CA and its sub CAs in the ISO 15118 context.

8.3. V2G Root CA

The V2G Root CA serves as main trust anchor within the Plug&Charge ecosystem. The operator of the V2G Root CA is obliged to fulfil the following tasks:

- Registration, validation and certification of underlying Sub-CAs
- Creation and revocation of certificates including the V2G Root and CPS and CPO sub CA certificates
- Operation of "*Online Certificate Status Protocol*" (OCSP) and "*Certificate Revocation List*" servers for the certificates, which are created by the V2G Root.
- Operation of a Root Certificate Pool as central instance for exchange of the OEM, MO and V2G Root certificates.
- Operation of a directory service for contracts (CCP) and OEM provisioning certificates (PCPs).
- Signing the contracts in the Certificate Provisioning Services.

8.4. OEM Root CA

The OEM Root CA is the trust anchor of the OEMs EVs, optionally same tasks may be fulfilled by an underlying OEM Sub-CA of the V2G Root CA:

- Distribution of public OEM Root CA Cert to the Root Certificate Pool (only applies to OEM Root CA).
- Creation of OEM Provisioning Certificates and link to corresponding unique PCID of vehicles
- Distribution of created OEM Provisioning Certificates to the PCP

8.5. MO Root CA

The MO Root CA is the trust anchor of the MO, optionally the same tasks may be fulfilled by an underlying MO Sub-CA of the V2G Root CA:

- Distribution of MO Root CA certificate in the Root Certificate Pool (only applies to MO Root CA).
- Creation of MO contract certificates and link to corresponding e-Mobility account identifier (EMAID) of customers
- Distribution of contract data to CPS for signing.

8.6. CPO Sub-CA

The ISO 15118 does not foresee a dedicated CPO Root CA, therefore CPOs are obliged to operate an underlying Sub-CA of the V2G Root. The operator of the CPO Sub-CA must to fulfil following tasks:

- Creation of EVSE Leaf Certificates and link to corresponding EVSEID
- Distribution of EVSE Leaf Certificates to SECCs

8.7. Provisioning Service Sub-CA

The Provisioning Service Sub-CA signs the leaf provisioning certificate, which is used in the CPS for the signing of the contract data. The CPS Sub-CAs are obliged to be an underlying Sub-CA of the V2G Root and can be operated by the V2G Root operator.

This signature can be validated in the EV to ensure that the data is not changed corrupted in the transport.

8.8. PCID and EMAID

Authentication of the EV at the charging station with Plug&Charge always refers to an active contract with an MO. The so-called e-Mobility Account Identifier (eMAID), which represents a charging contract number, is used as a reference to a charging contract. It is 18 characters long and defined in Appendix H of ISO 15118-2:2014. The Provisioning Certificate ID (PCID) of the vehicle is used to identify the vehicle when signing an assign traction power contract.

8.9. Usage of Root CA Certificates

OEM Root CA Certificate: Securing the processes from the OEM backend, especially for the insertion of the vehicle certificate, but also its revocation.

V2G Root CA Certificates: Trust anchor for establishing a TLS-secured connection to the charging station and validation of the origin of the contract package.

The OEM Root CA certificate is required to secure the insertion and deletion of the vehicle certificate as well as to update root CA certificates via a signed Root CA certificate container. Initially, an OEM Root CA certificate is already included in the Plug&Charge software.

The list of V2G Root CA certificates represents the trust anchor for public charging stations for the vehicle. The vehicle can use the V2G Root CA certificate to check the chain of certificates of the public charging station. The list of V2G root CA certificates must be compiled by a suitable (group) committee at regular intervals (e. g. annually). If a V2G root CA is compromised, a quick update must be done by removing the compromised provider.

8.10. Usage of Certificates Pools

Timing restriction for an end-to-end authentication from the MO to the EV (driver) is considered as the biggest technical challenge within the ISO 15118. As of today, the standard requires an end to end authentication within 5 seconds. Longer authentication processes will result into a timeout and re-triggering of the authentication which eventually leads into an “authentication loop”.

With the objective of solving this technical threshold, the Plug&Charge implementation rule proposed the introduction of pools which act as buffer for the authentication process. From a functional perspective, these pools are similar to today's UID / EVCOID whitelists or webservices.

Within the Plug&Charge ecosystem, three pools are necessary:

Pool	Description	Purpose	Advantage
Root Certificate Pool - RCP	RCP stores and provides the root certificates of the ISO 15118 participants.	RCP serves as a central storage of the root certificates.	ISO 15118 participants don't need to request root certificates from multiple resources.
Provisioning Certificate Pool - PCP	PCP stores OEM provisioning certificates of the EVs. Theses certificates (incl. sub CA certificates) must be delivered upon a valid MO request	PCP serves as an exchange point between the OEMs and MOs	MOs do not need to request OEM provisioning certificates from each OEM.
Contract Certificate Pool - CCP	CCP stores and publishes signed contract data for the OEM and CPO backend	Distribution of the signed contract data to CPO or OEM IT backend.	CCP serves as buffer for the MO Contract Certificate Installation Process. CPO / OEM IT Backend therefore are not required to request multiple MOs for creation of an MO Contract Certificate (1:1 instead of 1:n connection)

Table 1 – Description of pools

8.11. Online Certificate Status Protocol

To determine whether a certificate is still valid, the expiration date is used first. However, a certificate can also be revoked before it expires and thus become invalid. The EV must therefore be able to have the validity of a certificate confirmed by the issuer. The Online Certificate Status Protocol (OCSP, IETF RFC 6960) is used for this purpose.

The OCSP is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. The major advantage of the OCSP is that the client (e.g. the EVCC) can query the status of a single certificate, rather than having to download and parse an entire list which induces much less overhead on the client and network. OCSP can

be applied as an extension of an X.509 certificate, by using the Authority Information Access extension. This extension may be included in leaf or CA certificates.

The charging station then sends the signed OCSP Responses for all certificates in the selected certificate chain. The individual OCSP responses are signed by the respective issuing CA or a delegated OCSP responder. These OCSP Responses are cached by the charging station for a certain period of time (week is suggested). If the OCSP signature cannot be validated with the public key of the issuing CA (delegated OCSP responder), then the certificate of this OCSP responder must be included in the OCSP response. This certificate must be signed directly by the issuing CA and marked with a special extended key usage flag (IETF RFC 2560).

9. Processes

All processes of Plug&Charge described in ISO 15118 as "Certificate Provisioning" can be found in Section 7.9.2.5 (ISO 15118 – 2:2014) and explained in more detail in Appendix E. 3 (ISO 15118 – 2:2014).

The VDE Application Rule 2802 focusses on the processes and details each process flow for further understanding. Figure 2 shows the overall process with components and flows, which are based on the VDE Application Rule.

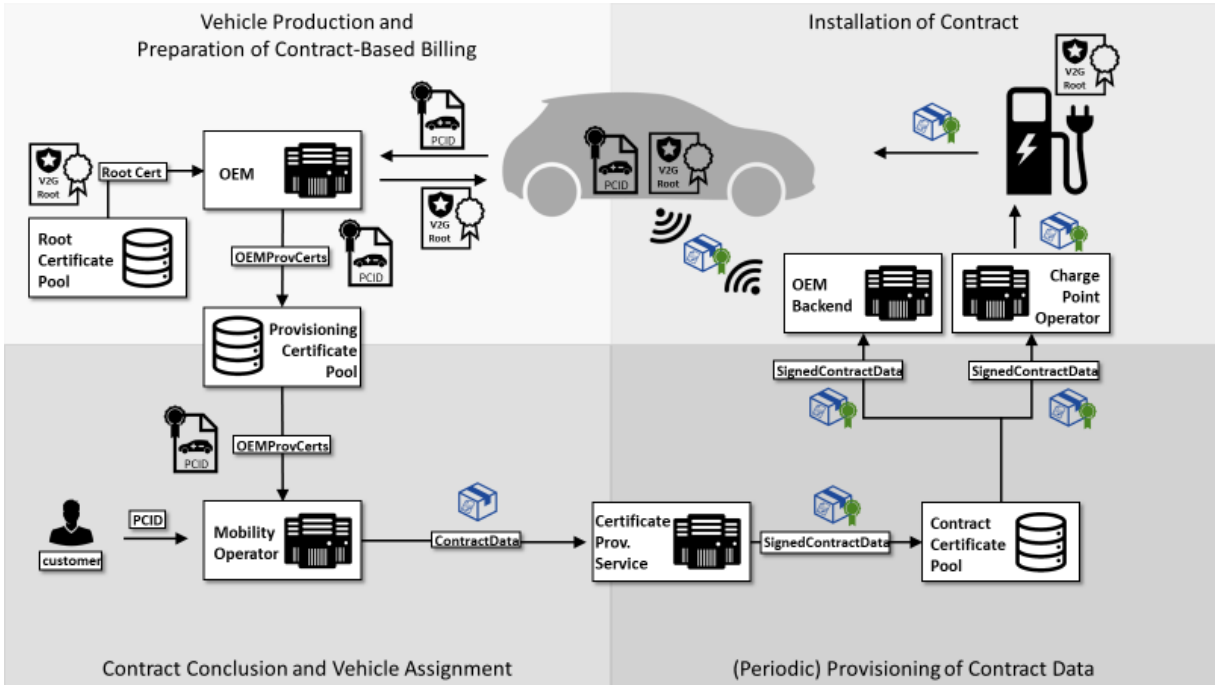


Figure 2 – The Application Rule process overview

The VDE Application Rule proposes the following sub processes.

Vehicle production and preparation of contract-based billing

a. Providing root certificates for public charging and contract-based billing
b. Production of vehicles and storing provisioning certificate

Contract conclusion and vehicle assignment

a. Conclusion of a contract with customer and receiving vehicle certificate from the vehicle certificate pool
b. Providing contract data to the Certificate Provisioning Service

(Periodic) Provisioning of contract data

a. Signing contract data and storing in the CCP

Installation of contract

a. Providing signed contract data to CPO-backend on request
b. Delivery of signed contract data to OEM-backend
c. Providing signed contract data as PKCS file to customer

Further information about the sub processes for each role is detailed in the following chapters.

9.1. Providing Root Certificates for Public Charging and Contract-Based Billing

The mutual trust between participants is a precondition for ISO 15118. For this purpose, a Root Certificate Pool is set up for all Root certificates. Each participant has access to and can receive the Root certificates of other participants to validate the trust chain of each certificate.

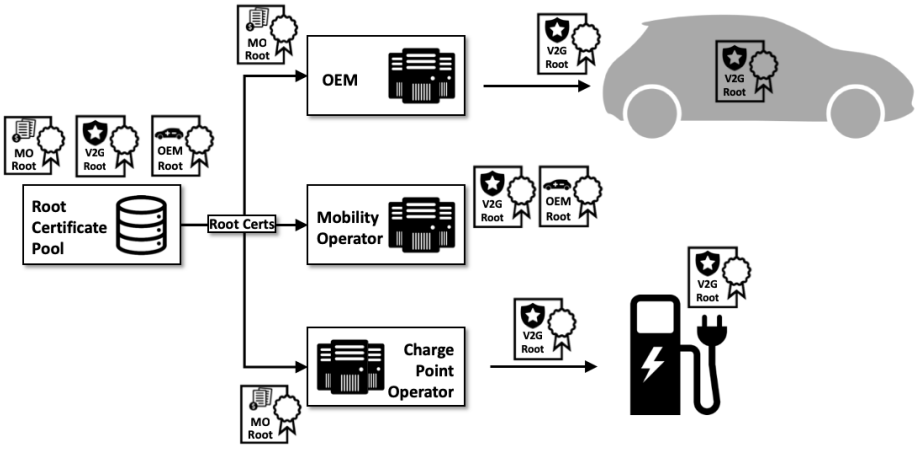


Figure 3 – Providing root certificates for public charging and contract-based billing

9.2. Production of Vehicles and Storing Provisioning Certificate

With the production of the vehicle, the OEM must create a provisioning certificate for each vehicle with a unique provisioning certificate identifier – PCID. The OEM sends this unique OEM provisioning certificate corresponding subordinate CA certificates to the Provisioning Certificate Pool securely.

The new EV owner must receive the PCID of its vehicle from the OEM at time of acquisition. Then the EV owner will give it to the MO when the two conclude a contract for EV charging services.

The required V2G root certificates must also be installed and stored in the vehicle for the trusted communication with charging devices.

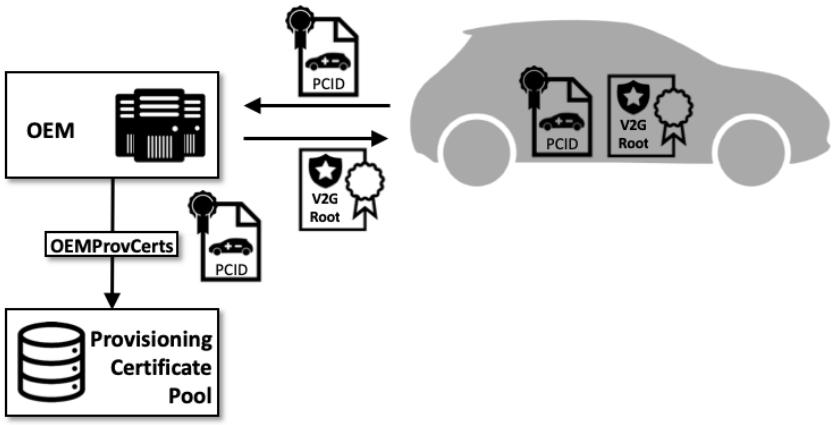


Figure 4 – Production of vehicles and storing provisioning certificate

9.3. Conclusion of contract with customer and receiving vehicle certificate from the provisioning certificate pool

This process describes, the conclusion of contract between customer and MO and delivery of OEM provisioning certificate of vehicle to the MO.

The MO must receive the contract information from a customer including the PCID of the vehicle. The PCID must be sent by the MO to the PCP. The PCP delivers OEM provisioning certificate, including the corresponding sub CA chain (See Figure 5).

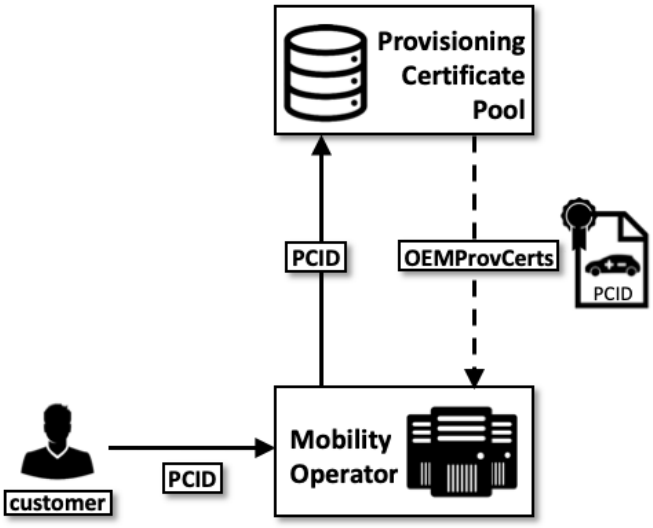


Figure 5 – Conclusion of contract and receiving vehicle certificate from vehicle certificate pool

After the verifying the authenticity of the trust chain with the OEM root certificate (which can be received from the Root Certificate Pool), the MO can generate a unique e-mobility account identifier for this contract.

9.4. Providing contract data to the Certificate Provisioning Service

The MO creates a contract data with the following information and sends to the Certificate Provisioning Service for signing:

- contractSignatureCertChain,
- dhPublicKey,
- contractSignatureEncryptedPrivateKey,
- EMAID

The Certificate Provisioning Service verifies the contract data and signs it. The purpose of signing the contract data by the V2G operator is, to guarantee that the contract data has not been altered or corrupted since it was signed. The EV can validate the signature with the V2G Root certificate, which is already stored in the EV.

The signed contract data will be stored in the Contract Certificate Pool (CCP) for the installation into the EVs.

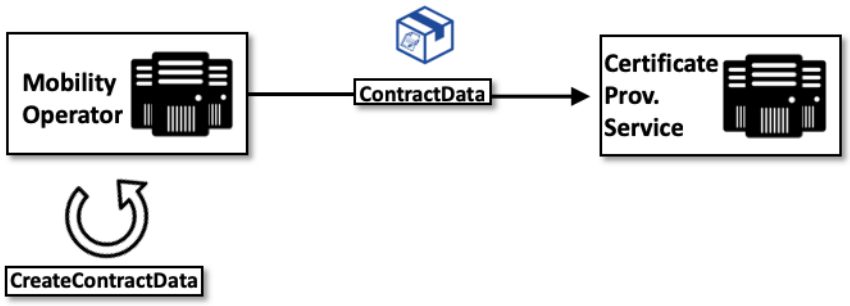


Figure 6 – Providing contract data to the Certificate Provisioning Service

9.5. Signing contract data and storing in the CCP

The Certificate Provisioning Service signs the following elements of the contract data:

- ContractSignatureCertChain
- ContractSignatureEncryptedPrivateKey
- DHPublicKey
- EMAID

and include the certificate chain of the provisioning certificate for the verification of this signature. The signed contract data converted to EXI format, before the storing in the CCP. The exact format of the signed contract data can be found in the ISO 15118 – 2:2014[13].

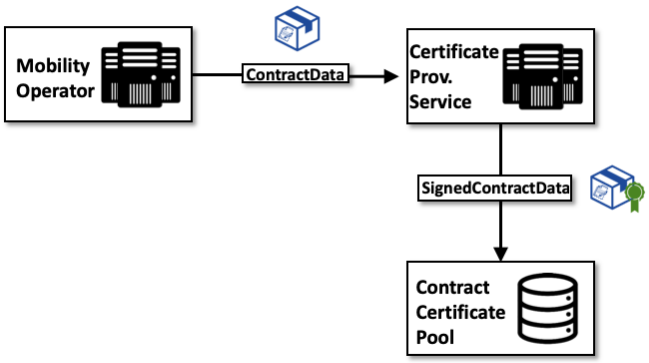


Figure 7 – Signing contract data and storing in the CCP

9.6. Providing signed contract data to CPO backend on request

There are two possibilities for the online installation of the signed contract data into the EV, sending it through the OEM backend or installation via EVSE.

After a successful handshake between EV and charging device, the EV sends a certificateInstallationRequest[14] to the charging device, which will be forwarded via the CPO backend to the CCP.

The CCP delivers the signed contract data of the vehicle, after the successful verification of the signature of the certificateInstallationRequest and the validity of each certificate.

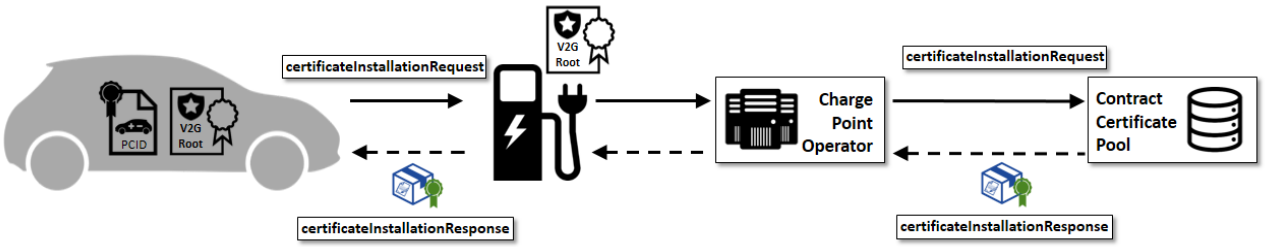


Figure 8 – Providing signed contract data to CPO backend on request

[13] ISO 15118 – 2:2014 Annex C
[14] ISO 15118 – 2:2014 Annex C

9.7. Delivery of signed contract data to OEM backend

The signed contract data can also be delivered to the EVs via the backend of OEMs. After the signing and storing of the signed contract data ("certificateInstallationRes") in the CCP, the CCP sends the signed contract data to the OEM for the delivery into the EV via Over-the-Air functionality.

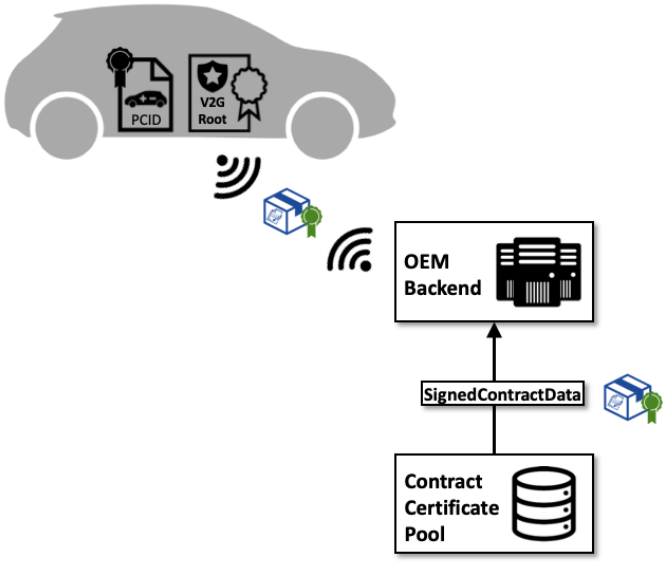


Figure 9 – Delivery of signed contract data to OEM backend

9.8. Provide signed contract data as PKCS file to customer

As an alternative to the installation processes of the signed contract data via CPO or OEM backend, ISO 15118 – 2:2014 describes an offline certificate installation process[15]. If the necessary infrastructure is not available or the EV doesn't support the "certificateInstallationReq/Res" communication, the signed contract data can be delivered to the customer (e.g. per post, email) and stored in the EV with using an interface, such as diagnosis interface or internet access to the EV.

[15] ISO 15118 – 2:2014, Chapter 8.4.3.11.4

10. Use cases

10.1. Introduction

Use cases describe the methods how a user can adopt the VDE application sub processes. The use cases mentioned in this chapter are a list of actions or steps typically defining interactions between the roles (OEM, CPO, MO) to be compliant to ISO 15118 standard. The actions are based on the VDE application sub processes. The general use case defines the goal, pre-conditions, actors involved, scenario of application and post-conditions.

10.2. Relevant Use Cases for OEMs

The OEMs could cover the following use cases in relation to ISO 15118:

1. Manage the lifecycle of OEM certificates in OEM CA
2. Manage the lifecycle of OEM certificates in EV
3. Provide the OEM provisioning certificates to the Provisioning Certificate Pool
4. Store V2G Root certificate in EV
5. Installation of signed contract data in the EV
6. Optional: Receive and store MO Root certificates in EV

10.2.1. Manage the Lifecycle of OEM Certificates in OEM CA

UC Name	OEM 1 – Manage the lifecycle of the OEM certificates in OEM CA
Goal in the context	OEM generates the necessary certificates for the public charging preparation with ISO 15118. All ISO 15118 certificates must be created as defined in the ISO 15118 – 2:2014 standard.
Preconditions	• OEM owns a public key infrastructure, incl. certificate manager software and HSM device. • Unique PCID for the EV
Actors	OEM
Main Scenario	1. OEM generates a key pair, public and private keys. 2. OEM creates a certificate signing request (CSR) with the public key and signs it with the private key to create a self-signed OEM Root certificate 3. OEM generates a key pair and creates a CSR with public key and signs it with OEM Root CA private key to create an OEM sub 1 CA certificate 4. Optional: OEM generates a key pair and creates a CSR with public key and signs it with OEM sub 1 CA private key to create an OEM sub 2 CA certificate 5. OEM or EV generates a key pair and creates a CSR with the public key and signs it with the private key of the OEM sub 2 CA to create an OEM provisioning certificate
Postconditions	• OEM Root CA and OEM Root CA certificate is created • OEM sub 1 CA and OEM sub 1 CA certificate is created • OEM sub 2 CA and OEM sub 2 CA certificate is created • OEM provisioning certificate is created

Table 2 – Manage the lifecycle of the OEM provisioning certificates in OEM CA

10.2.2. Manage the Lifecycle of OEM Certificates in EV

UC Name	OEM 2 – Manage the lifecycle of the OEM certificates in EV
Goal in the context	OEM CA stores the certificates, which are necessary for the public charging with ISO 15118. All ISO 15118 certificates must be created as defined in the ISO 15118 – 2:2014 standard.
Preconditions	• OEM owns a public key infrastructure, incl. certificate manager software and HSM device. • OEM Root CA, sub 1 CA and optionally sub 2 CA certificates are created • OEM provisioning certificate is created with unique PCID
Actors	OEM
Main Scenario	1. OEM generates a key pair 2. OEM creates a CSR with the public key of the key pair 3. OEM signs the CSR with OEM sub 1 CA or if available with sub 2 CA private key and creates an OEM provisioning certificate 4. OEM stores the OEM provisioning certificate in the EV.
Postconditions	OEM provisioning certificate stored in EV

Table 3 – Manage the lifecycle of the OEM certificates in EV

10.2.3. Provide the OEM Provisioning Certificates to the PCP

UC Name	OEM 3 – Provide the OEM provisioning certificates to the PCP
Goal in the context	Storing the OEM provisioning certificates of the EVs in the PCP
Preconditions	• OEM Root, sub 1 and if available sub 2 CA certificates are created • OEM provisioning certificate with unique PCID created • Optionally: OEM Root, sub 1, sub 2 CA certificates are stored in the EV • OEM provisioning certificate is stored in the EV • Interface between OEM and PCP is implemented
Actors	OEM, V2G Root operator
Main Scenario	1. OEM sends OEM provisioning certificate, sub 1 certificate and if available sub 2 certificate to the PCP 2. PCP validates the certificates 3. PCP stores the certificates
Postconditions	• OEM sub 1 CA certificate stored in the PCP • If available: OEM sub 2 CA certificate stored in the PCP • OEM provisioning certificate stored in the PCP

Table 4 – Provide the OEM provisioning certificates to the PCP

10.2.4. Store V2G Root certificate in EV

UC Name	OEM 4 – Store V2G Root certificate in the EV
Goal in the context	Storing V2G Root certificate in EVs for the secure and trusted communication between EVs and EVSEs
Preconditions	• V2G Root operator created V2G Root certificate • V2G Root operator published V2G Root certificate in the Root Certificate Pool
Actors	OEM, V2G Root operator
Main Scenario	1. OEM requests V2G Root certificate from V2G Root operator 2. OEM receives V2G Root certificate from V2G Root operator 3. OEM checks the validity of V2G Root certificate 4. OEM stores V2G Root certificate in EVs
Postconditions	V2G Root certificate stored in EVs

Table 5 – Store V2G Root certificate in the EV

10.2.5. Installation of Signed Contract Data to EV

UC Name	OEM 5 – Installation of signed contract data in the EV
Goal in the context	Installation of signed contract data (certificateInstallationRequest) into EV for starting the charging process with ISO15118
Preconditions	• OEM produced an ISO 15118 compatible EV • OEM created and stored OEM root, sub 1, sub 2 CA and OEM provisioning certificates • OEM stored OEM Root certificate in root certificate pool • OEM published OEM sub 1, OEM provisioning certificates and optionally sub 2 CA certificate in the PCP • Customer delivered the PCID of EV to MO • Customer and MO concluded a contract • Mobility operator requested the OEM sub 1, sub 2 and OEM provisioning certificates from PCP with the customers PCID • Mobility operator generated a unique EMAID for the contract • MO created a contractData as described in ISO 15118 – 2:2014 • MO send contractData to Certificate Provisioning Service (CPS) for signing the contractData • CPS signed the contractData and stored in contract certificate pool • CPO stored V2G Root certificate, CPO sub 1 CA, CPO sub 2 CA and EVSE leaf certificate in EVSE • EVSE connected to the CPO backend • CPO backend connected to CCP
Actors	OEM, MO, PCP, CPS, CCP, CPO
Main Scenario	1. Customer plugs in an ISO 15118 compatible charging device into EV 2. EV generates a certificateInstallationReq 3. EV sends certificateInstallationReq to EVSE 4. EVSE sends certificateInstallationReq to CPO backend 5. CPO backend sends certificateInstallationReq to CCP 6. CCP checks the available signed contractData (certificateInstallationRes) for this EV 7. CCP delivers signed contractData to CPO backend 8. CPO backend delivers signed contractData to EVSE 9. EVSE installs signed contractData into EV and stores the private key of the contract in a secure module.
Postconditions	Charging process starts

Table 6 – Installation of signed contract data to EV

10.2.6. Optional: Receive and Store MO Root Certificates in EV

UC Name	OEM 6 – Receive and store MO Root certificates in EV
Goal in the context	If mobility operator doesn't use V2G Root CA as the highest trust anchor, MO Root certificate must be also stored in EV to validate contract certificate chain in EV.
Preconditions	• Mobility operator created its own MO Root CA • Mobility operator published MO Root certificate in root certificate pool
Actors	OEM, V2G Root operator, MO
Main Scenario	1. OEM requests MO Root certificate from root certificate pool 2. OEM receives MO Root certificate from root certificate pool 3. OEM checks the validity of MO Root certificate 4. OEM stores MO Root certificate in EVs
Postconditions	MO Root certificate stored in EVs

Table 7 – Optional: Receive and Store MO Root certificates in EV

10.3. Relevant Use Cases for MOs

The MOs cover the following use cases in relation to ISO 15118:

1. Conclusion of a Plug&Charge contract with customer
2. Receive the OEM provisioning certificate of the EV
3. Assign EV to contract
4. Create contract data for the costumer
5. Send contract data to the Certificate Provisioning Service (CPS)
6. Optional: Receive OEM Root certificates

10.3.1. Conclusion of a Plug&Charge contract with customer

UC Name	MO 1 – Conclusion of a Plug&Charge contract with customer
Goal in the context	The mobility operator sells a Plug&Charge contract to its customer.
Preconditions	• Customer has an ISO 15118 compatible EV • The EV driver has obtained the PCID from OEM or via functionality provided by the EV
Actors	Customer, MO
Main Scenario	1. Customer concludes contract with MO 2. Customer provides the PCID of his EV 3. MO stores the customer information and PCID in MO systems
Postconditions	• Customer information stored in MO system • PCID stored in MO systems

Table 8 – Conclusion of contract with customer

10.3.2. Receive the OEM provisioning certificate of the EV

UC Name	MO 2 – Receive the OEM provisioning certificate of the EV
Goal in the context	The mobility operator receives the OEM provisioning certificate and its chain from the PCP and verifies the validity and the chain.
Preconditions	• PCID of the customer's EV stored in MO system • OEM delivered the OEM provisioning certificate and the sub CA certificates of the EV to the PCP
Actors	MO, PCP
Main Scenario	1. MO sends the PCID to the PCP 2. The PCP delivers the OEM provisioning and corresponding sub CA certificates of the customers EV to the MO 3. MO stores the OEM provisioning certificate of the customer's EV 4. MO checks the validity of the certificates, from the OCSP responder or CRL distribution point of the OEM. 5. MO validates the chain of the certificates with the OEM Root certificate (see **Fehler! Verweisquelle konnte nicht gefunden werden.**)
Postconditions	OEM provisioning certificate and the corresponding sub CA certificates of the customer EV stored in MO system

Table 9 – Receive the OEM provisioning certificate of the EV

10.3.3. Assign EV to contract

UC Name	MO 3 – Assign EV to contract
Goal in the context	This use cases covers the operations the MO has to fulfill in order to assign an EV (PCID) to the e-mobility account of a contract (EMAID).
Preconditions	• The customer signed a contract with the MO for ISO 15118 functionality • The customer information and the PCID is already in the MO system • MO received the OEM provisioning and corresponding sub CA certificates from the PCP • MO verified the validity of the OEM provisioning and corresponding sub CA certificates
Actors	EV driver, MO, CPO
Main Scenario	MO generates a e-mobility account identifier (EMAID) for the contract of the customer
Postconditions	• The customer has an EMAID

Table 10 – Assign EV to contract

10.3.4. Create contract data for the customer

UC Name	MO 4 – Create contract data for the customer
Goal in the context	The mobility operator creates contract data to enable the customer EV for ISO 15118 charging.
Preconditions	• The customer has an EMAID • OEM provisioning certificate of the customers EV stored in MO system • OEM provisioning, sub 1 CA and sub 2 CA certificates are valid • Trust chain of the OEM provisioning certificate verified
Actors	MO, CPS
Main Scenario	1. MO creates a key pair (public and private key) for the contract lead certificate 2. MO generates a CSR with the public key of the contract leaf certificate and signs it with the private key 3. MO sends the CSR to the MO sub 2 CA to create a contract leaf certificate 4. MO sub 2 CA creates a contract certificate with the common name EMAID of the customer 5. MO receives MO sub 1 and sub 2 CA certificates from MO CA 6. MO generates DHPublicKey with OEM provisioning certificate of the EV 7. MO encrypts the private key of the contract leaf certificate with the DHPublicKey 8. MO creates a contract data, as defined in ISO 15118 – 2:2014
Postconditions	MO generated a contract data

Table 11 – Create contract data for the customer

10.3.5. Send contract data to the Certificate Provisioning Service (CPS)

UC Name	MO 5 – Send contract data to the Certificate Provisioning Service (CPS)
Goal in the context	The mobility operator sends the contract data to CPS to be signed. The EV uses the signature of the contract data for the validation.
Preconditions	MO has access to the Contract Provisioning Service (CPS)
Actors	MO, CPS
Main Scenario	1. MO sends the contract data to the CPS 2. The CPS validates the delivered contract data 3. The CPS adds the Provisioning leaf, sub 2 and sub 1 CA certificates in the contract data 4. The CPS signs the contract data 5. The CPS sends the signed contract data to the CCP 6. The CCP stores the signed contract data for the provisioning to the CPOs and validation by the EV when a charging event occurs. 7. Optionally: the CCP sends the signed contract data to the OEM backend to be transmitted to the EV
Postconditions	The signed contract data stored in the CCP.

Table 12 – Send contract data to the Certificate Provisioning Service (CPS)

10.3.6. Optional: Receive OEM Root certificates

UC Name	MO 6 – Optional: Receive OEM Root certificates
Goal in the context	The mobility operator receives the root certificate of the OEM to validate the trust chain of the OEM provisioning certificate
Preconditions	MO has access to the Root Certificate Pool (RCP)
Actors	MO, RCP
Main Scenario	1. MO sends the root certificate ID of the OEM Root certificate to the RCP 2. MO receives the root certificate of the OEM
Postconditions	MO stored the root certificate of the OEM

Table 13 – Optional: Receive OEM Root certificates

10.3.7. Optional: Provide Signed Contract Data as PKCS File to Customer

UC Name	MO 7 – Optional: Provide signed contract data as PKCS file to customer
Goal in the context	As an option, the mobility operator can send the contract data to the CPS for signing and receive a signed contract data. The signed contract data can be delivered to the customer (e.g. per post, email) and stored in the EV with using an interface, such as diagnosis interface or internet access to the EV.
Preconditions	• The customer has a contract with the MO • MO created a contract data for the customer (as defined in ISO 15118 – 2:2014) • The contract data signed by the CPS and delivered back to the MO
Actors	MO, customer
Main Scenario	1. MO sends the signed contract data in a secured form (e.g. pkcs#12) to the customer. 2. Customer installs the signed contract data into the ISO 15118 compatible EV
Postconditions	The signed contract data installed in the EV of the customer

Table 14 – Optional: Receive OEM Root certificates

10.4. Relevant Use cases for CPOs

The CPOs cover the following functions in relation to ISO 15118 and the Ecosystem:

1. Manage the lifecycle of EVSE leaf certificates
2. Store V2G Root certificate in EVSE
3. Installation of signed contract data into EV (EVCC)

10.4.1. Manage the Lifecycle of EVSE Leaf Certificates

UC Name	CPO 1 – Manage the lifecycle of the EVSE leaf certificates
Goal in the context	EVSE certificates corresponding to CPO sub 1 and sub 2 CA must be created and stored in the EVSE to start a secure communication between EV (EVCC) and charging device (SECC). All ISO 15118 certificates must be created as defined in the ISO 15118 – 2:2014 standard.
Preconditions	• CPO installed an ISO 15118 capable charging device (EVSE). • EVSE connected to the CPO backend. • CPO backend connected to the EST interface of V2G Root operator. • Unique EVSEID for the EVSE • V2G Root, CPO sub 1 and sub 2 CA certificates installed in the EVSE
Actors	EVSE, CPO-backend, V2G Root operator
Main Scenario	1. EVSE generates a key pair, public and private keys 2. EVSE creates a certificate signing request (CSR) with the public key and signs it with the generated private key 3. EVSE sends the CSR to the CPO-backend 4. CPO backend forwards the CSR to the EST interface of the V2G Root operator 5. V2G Root operator signs the CSR with the private key of the CPO sub 2 CA, and sends as a CPO leaf certificate back to the CPO backend 6. CPO backend forwards the EVSE leaf certificate to the EVSE 7. EVSE stores the EVSE leaf certificate
Postconditions	• EVSE leaf certificate stored in the EVSE

Table 15 – Manage the lifecycle of the EVSE leaf certificates

10.4.2. Store V2G Root Certificate in EVSE

UC Name	CPO 2 – Store V2G Root certificate in EVSE
Goal in the context	Storing V2G Root certificate as a trust anchor in charging device (EVSE).
Preconditions	• CPO installed an ISO 15118 capable charging device (EVSE). • EVSE connected to the CPO backend. • V2G Root, CPO sub 1 and sub 2 CA certificates installed in the EVSE
Actors	EVSE, CPO-backend, V2G Root operator
Main Scenario	1. CPO receives the V2G Root certificate from the Root Certificate Pool 2. CPO stores the V2G Root certificate during the initial setup of the EVSE
Postconditions	V2G Root certificate stored in the EVSE

Table 16 – Store V2G Root certificate in EVSE

10.4.3. Installation of Signed Contract Data into EV (EVCC)

UC Name	CPO 3 – Installation of signed contract data into EV (EVCC)
Goal in the context	Installation of the signed contract data to start the ISO 15118 based public charging.
Preconditions	• CPO installed an ISO 15118 capable charging device (EVSE). • EVSE connected to the CPO backend. • CPO backend connected to the CCP interface of V2G Root operator. • V2G Root, CPO sub 1 and sub 2 CA and EVSE leaf certificates installed in the EVSE • ISO 15118 compatible EVCC built in the EV • V2G Root certificate stored in the EV • OEM provisioning, sub 1 CA and sub 2 CA certificates stored in the EV • Signed contract data stored in the Contract Certificate Pool (CCP)
Actors	EV, charging device (EVSE), CPO-backend, CCP
Main Scenario	11. TLS handshake between EV (EVCC) and charging device (SECC) completed successfully 11. EV generated a “certificateInstallationReq” with the OEM provisioning certificate and list of the root IDs 11. EV sends the “certificateInstallationReq” to the EVSE 11. EVSE sends the “certificateInstallationReq” to the CPO backend 11. CPO backend forwards the “certificateInstallationReq” to the CCP 11. CCP controls the signature of the “certificateInstallationReq” 11. CCP delivers all the available signed contracts (“certificateInstallationRes”) of the EV to the CPO backend 11. CPO backend forwards the signed contract data to the EVSE 11. EVSE installs the signed contract data (“certificateInstallationReq”) into the EV
Postconditions	• Signed contract data (“certificateInstallationReq”) installed into the EV

Table 17 – Installation of signed contract data into EVSE

11. Requirements

11.1. Requirements for OEMs

Plug&Charge control unit in EV (EVCC)

- Support of charge communication according to ISO 15118 – 2:2014 incl. Plug&Charge and TLS connection
- Support of cryptographic functions
- Secure module for the storing of the private key of the OEM provisioning certificate in EV
- Certificate management and delivery
- Interface to the SECC

Connectivity Unit (CU) in EV (Optional)

- Over the Air connection between EV and OEM backend for certificate management
- Over the Air connection between EV and OEM backend for the installation of signed contract data

Plug&Charge display control unit (Optional)

- Display and operation (activate/deactivate) of the Plug&Charge function in the vehicle HMI, central display and instrument cluster
- Display and operation of (trigger) installation of a new contract certificate for Plug&Charge

OEM backend (Optional)

- Interface to the Plug&Charge Remote Service on the CU in the vehicle (air interface)
- Interface to OEM CA for certificate management
- Interface to the Contract Certificates Pool

OEM CA (Optional)

- Certificate software for EV certificates
- Interface to the provisioning certificate pool
- Interface to V2G Root CA

OEM customer portal (Optional)

- Customer frontend - sales platform for traction power contracts
- Display and operation (activate/deactivate) of the Plug&Charge function in the OEM customer portal
- OEM App
- Display and operation (activate/deactivate) of the Plug&Charge function in the OEM App

11.1.1. Required messages

The messages, containing the data structures and data types, which need to exchange between the EVCC and SECC are presented in XML files, using XSD files. DIN EN ISO 15118 – 2:2014 lists the following XSD files needed for message exchange. [16]

- V2G_CI_AppProtocol.xsd (Defines the protocol handshakes)
- V2G_CI_MsgDef.xsd (Defines the message structure)
- V2G_CI_MsgHeader.xsd (Defines the message header)
- V2G_CI_MsgBody.xsd (Defines the message body)
- V2G_CI_MsgDataTypes.xsd (Defines the datatypes)
- Xmldsig-core.schema.xsd (defines the schema for XML signatures)

[16] VDE-AR-E 2802-100-1:2017-120 (en)

11.2. Requirements for MOs

MO customer portal

- Customer frontend and app for the sales platform for traction power contracts
- Display and operation (activate/deactivate) of the Plug&Charge function in the OEM customer portal
- Display and operation (activate/deactivate) of the Plug&Charge function in the MO App

MO CA

- Certificate software for EV certificates
- Interface to the provisioning certificate pool
- Interface to V2G Root CA
- Interface to the CPS

11.2.1. Required messages

The messages, containing the data structures and data types, which need to exchange between the EVCC and SECC are presented in XML files, using XSD files. DIN EN ISO 15118 – 2:2014 lists the following XSD files needed for message exchange. [17]

- V2G_CI_AppProtocol.xsd (Defines the protocol handshakes)
- V2G_CI_MsgDef.xsd (Defines the message structure)
- V2G_CI_MsgHeader.xsd (Defines the message header)
- V2G_CI_MsgBody.xsd (Defines the message body)
- V2G_CI_MsgDataTypes.xsd (Defines the datatypes)
- Xmldsig-core.schema.xsd (defines the schema for XML signatures)

All the above mentioned schemas can be downloaded from the open-source RISE V2G open-source project, via: https://github.com/V2GClarity/RISE-V2G/tree/master/RISE-V2G-Shared/src/main/resources/schemas

[17] VDE-AR-E 2802-100-1:2017-120 (en)

11.3. Requirements for CPOs

11.3.1. Generic ISO 15118 requirements

- EVSE must be ISO 15118 capable
- CPO must install the V2G Root certificate into EVSE.
- CPO must install EVSE leaf, CPO sub 1 and CPO sub 2 CA certificates into EVSE
- EVSE must have a unique EVSEID
- The Mobility Operator must provide the contract package so that it can be installed in the vehicle.
- The charging station operator must install the charging station certificate in his charging stations.

11.3.2. Specific requirements for CPOs

Electric Vehicle Supply Equipment

- Support of charge communication according to ISO 15118 – 2:2014 incl. Plug&Charge and TLS connection
- Support of cryptographic functions
- Secure module for the storing of the private key of the EVSE leaf certificate
- Certificate management functionality (creating and sending CSR)
- Retrieving sub CA certificates from V2G operator.
- Interface to the CPO backend
- Optional: Sending OCSP request, receiving OCSP response
- Optional: Calling CRL distribution point and reading CRL

CPO backend

- Interface to the EVSEs
- Interface to the Contract Certificate Pool (CCP)

11.3.3. Required messages

The messages, containing the data structures and data types, which need to exchange between the EVCC and SECC are presented in XML files, using XSD files. DIN EN ISO 15118 – 2:2014 lists the following XSD files needed for message exchange. [18]

- V2G_CI_AppProtocol.xsd (Defines the protocol handshakes)
- V2G_CI_MsgDef.xsd (Defines the message structure)
- V2G_CI_MsgHeader.xsd (Defines the message header)
- V2G_CI_MsgBody.xsd (Defines the message body)
- V2G_CI_MsgDataTypes.xsd (Defines the datatypes)
- Xmldsig-core.schema.xsd (defines the schema for XML signatures)

All the above mentioned schemas can be downloaded from the open-source RISE V2G open-source project, via: https://github.com/V2GClarity/RISE-V2G/tree/master/RISE-V2G-Shared/src/main/resources/schemas

[18] VDE-AR-E 2802-100-1:2017-120 (en)

12. References

- [ISO/IEC15118-1] ISO 15118-1 specifies terms and definitions, general requirements and use cases as the basis for the other parts of ISO 15118. It provides a general overview and a common understanding of aspects influencing the charge process, payment and load leveling. https://webstore.iec.ch/publication/6029
- [ISO/IEC15118 – 2:2014] Road vehicles – Vehicle to grid communication interface – Part 2: Technical protocol description and Open Systems Interconnection (OSI) layer requirements, Document Identifier: 69/216/CDV. https://webstore.iec.ch/publication/9273
- ISO 15118 Manual, Dr. Marc Mültin. https://www.v2g-clarity.com/en/iso15118-masterclass/
- VDE-AR-E 2802-100-1:2018-120 (EN) Handling of certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO 15118 English translation of VDE-AR-E 2802-100-1:2017-10
- ISO/IEC 27000 family - Information security management systems https://www.iso.org/isoiec-27001-information-security.html
- IEC: IEC 61851-1 ed2.0: Electric vehicle conductive charging system - Part 1: General requirements URL: http://webstore.iec.ch/webstore/webstore.nsf/Artnum_PK/44636

13. About Hubject GmbH

Hubject was founded in 2012 by leading companies from the energy, technology and automotive industry: BMW Group, Bosch, Daimler, EnBW, innogy and Siemens, later joined by the Volkswagen Group as a 7th shareholder in 2017. Since its creation, Hubject's B2B e-Roaming Platform enables real-time connections between European charge point operators and e-Mobility service providers and provides cross-operator access to European charging stations with only one contract and one interface. With more than 300 partners, the Hubject e-Roaming Platform is the largest international digital B2B market place for services related to charging of electric vehicles. Hubject provides ISO 15118 related products and services and e-Mobility consulting services.

14. Glossary

CA	Certification authority
CP	Certificate policy
CCP	Contract Certificate Pool (webservice)
CPS	Certification practice statement (document)
CPS	Certificate Provisioning Service (webservice)
CRL	Certificate Revocation List
DN	Distinguished Name
EE	End-entity
EV	Electric Vehicle
EVCC	Electric Vehicle Communication Controller
EVSE	Electric Vehicle Supply Equipment; practically a charge point
ISO	International Organization for Standardization
MO	Mobility Operator (e-Mobility Service Provider)
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer of an Electric Vehicle
PKI	Public Key Infrastructure
RFC	Request for Comment
SECC	Supply Equipment Communication Controller; the supply equipment is practically a charge point
Sub-CA	Subordinate CA
TLS	Transport Layer Security

Table 18 - Glossary

15. Annexes

Annex I - Mapping table to OCPP 2.0

Implementation Guide	ISO 15118	OCPP 2.0
	Provisioning	
	A1 Begin of charging process with forced High Level Communication	
	A2 Begin of charging process with concurrent IEC 61851-1 and High Level Communication	
	B1 EVCC/SECC communication setup	
Certificate Management	**Certificate Management**	
V2G ROOT CA	C1 Certificate update	OCPP 2.0 E01 - Certificate Update
OEM PROVISIONING CERTIFICATE	C2 Certificate installation	OCPP 2.0 E02 - Certificate Installation
EVSE LEAF CERTIFICATE INSTALLATION		
MO CONTRACT CERTIFICATE INSTALLATION AND DISTRIBUTION VIA CABLE		
MO CONTRACT CERTIFICATE INSTALLATION AND DISTRIBUTION VIA TELEMATICS/OEM		
Authorization	**Authorization**	
AUTHENTICATION AND AUTHORIZATION	D1 Authorization using Contract Certificates performed at the EVSE	
	D2 Authorization using Contract Certificates performed with help of SA	OCPP 2.0 C14 - Authorization using Contract Certificates performed with the help of the Central System
	D3 Authorization at EVSE using external credentials performed at the EVSE	OCPP 2.0 C15 - Authorization using Contract external credentials at the Charge Point
	D4 Authorization at EVSE using external credentials performed with help of CA	OCPP 2.0 C16 - Authorization at EVSE using external credentials performed with help of the Central System
	Smart Charging	

	E1 AC charging with load levelling based on High Level Communication	
	E2 Optimized charging with scheduling to secondary actor	
	E3 Optimized charging with scheduling at EV	
	E4 DC charging with load levelling based on High Level Communication	
	E5 Resume to Authorized Charge Schedule	
	Charging loop	
	F0 Charging loop	
	F1 Charging loop with metering information exchange	
	F2 Charging loop with interrupt from the SECC	
	F3 Charging loop with interrupt from the EVCC or user	

Table 19 – Annex 1

Annex II – ISO 15118 Certificates

Certificate Structure refer to ISO 15118 – 2:2014 Annex E.1.5 Overview of the resulting certificate structure

Provisioning Service Certificates Profile
ISO 15118-2:2014 Table F.3 of Annex F

CPO Certificates Profile
ISO 15118-2:2014 Table F.2 of Annex F

MO Certificates Profile
ISO 15118-2:2014 Table F.4 of Annex F