M. ISO 15118 CertificateManagement

1. Introduction

The ISO/IEC JWG 15118 for the Vehicle to Grid Communication Interface (V2G CI) was founded in 2009 with means to the need of a complementary international standard to IEC 61851-1 [IEC61851-1] providing bi-directional digital communication based on Internet protocols. The major purpose of 15118 is to establish a more advanced and autonomously working charge control mechanism between EVs and charging infrastructures. The standard is currently under development and will ultimately provide means for various authentication schemes (e.g. plug charge vs. external identification means, like RFID cards), automatic handling of charging services as well as (proprietary) value added services, charge scheduling and advance planning, etc.

The 15118 standard is of interest to the Open Charge Alliance, as it provides the exchange of charging schedules and enables to control the amount of power that an EV may draw from a Charging Station, in which some form of vehicle to grid communication is necessary. Especially the second part, which specifies the messages to be exchanged between the communication partners (Application Layer), the associated data and data types (Presentation Layer) via TCP/IP based Transport and Network Layer, is important to acknowledge in this specification. The authorization for charging is provided either by External Identification Means (EIM), such as an RFID card, or by the Plug and Charge (PnC) mechanism using a contract certificate stored in the EV, handled by the certificate handling process in use case elements "C", eliminating the need of other authorization means.

This 15118 OCPP Functional Block has been designed to meet a number of alignment objectives:

- To allow the communication between an EV (BEV or a PHEV) and an EVSE.
- To allow the support of certificate-based authentication and authorization at the Charging Station, i.e. plug and charge.

For illustration purposes: the figure below shows a complete sequence with authorization and scheduling.

NOTE To the below figure: this sequence only applies for AC charging, although the certificate handling (which is the focus in this section) does not differ in AC or DC.

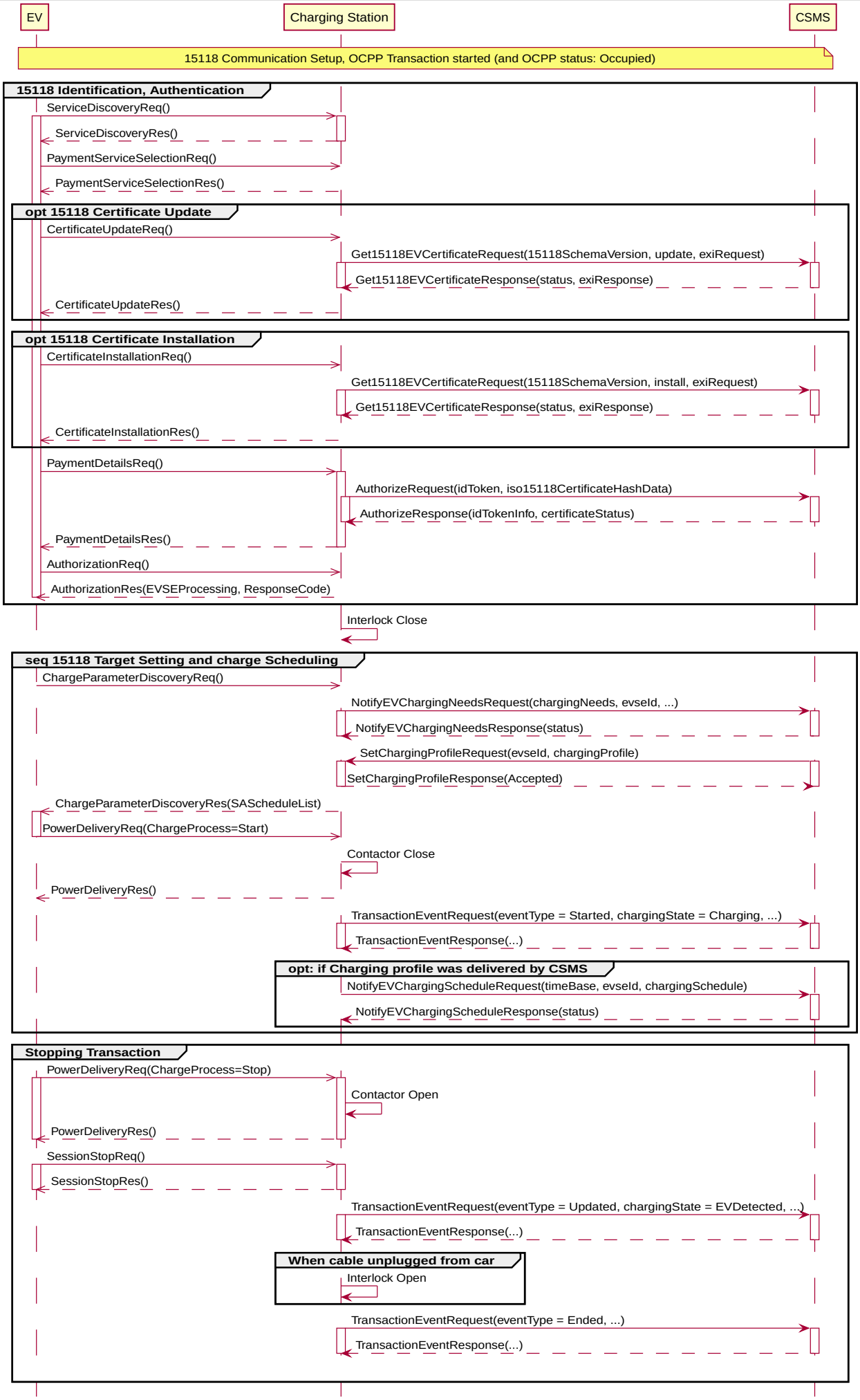
EV
Charging Station
CSMS
15118 Communication Setup, OCPP Transaction started (and OCPP status: Occupied)
15118 Identification, Authentication
ServiceDiscoveryReq()
ServiceDiscoveryRes()
PaymentServiceSelectionReq()
PaymentServiceSelectionRes()
opt 15118 Certificate Update
CertificateUpdateReq()
Get15118EVCertificateRequest(15118SchemaVersion, update, exiRequest)
Get15118EVCertificateResponse(status, exiResponse)
CertificateUpdateRes()
opt 15118 Certificate Installation
CertificateInstallationReq()
Get15118EVCertificateRequest(15118SchemaVersion, install, exiRequest)
Get15118EVCertificateResponse(status, exiResponse)
CertificateInstallationRes()
PaymentDetailsReq()
AuthorizeRequest(idToken, iso15118CertificateHashData)
AuthorizeResponse(idTokenInfo, certificateStatus)
PaymentDetailsRes()
AuthorizationReq()
AuthorizationRes(EVSEProcessing, ResponseCode)
Interlock Close
seq 15118 Target Setting and charge Scheduling
ChargeParameterDiscoveryReq()
NotifyEVChargingNeedsRequest(chargingNeeds, evseId, ...)
NotifyEVChargingNeedsResponse(status)
SetChargingProfileRequest(evseId, chargingProfile)
SetChargingProfileResponse(Accepted)
ChargeParameterDiscoveryRes(SAScheduleList)
PowerDeliveryReq(ChargeProcess=Start)
Contactor Close
PowerDeliveryRes()
TransactionEventRequest(eventType = Started, chargingState = Charging, ...)
TransactionEventResponse(...)
opt: if Charging profile was delivered by CSMS
NotifyEVChargingScheduleRequest(timeBase, evseId, chargingSchedule)
NotifyEVChargingScheduleResponse(status)
Stopping Transaction
PowerDeliveryReq(ChargeProcess=Stop)
Contactor Open
PowerDeliveryRes()
SessionStopReq()
SessionStopRes()
TransactionEventRequest(eventType = Updated, chargingState = EVDetected, ...)
TransactionEventResponse(...)
When cable unplugged from car
Interlock Open
TransactionEventRequest(eventType = Ended, ...)
TransactionEventResponse(...)

Figure 121. Sequence with Authorization and Scheduling

NOTE The time-out on the ChargeParameterDiscoveryReq is 2 seconds, but this can be prolonged up to 60 seconds to wait for charging profile to be provided by the CSMS. See ISO 15118-2 [ISO15118-2].

NOTE Please note that it is highly RECOMMENDED to use one of the TLS based security profiles from functional block A, not doing this might "break" the ISO 15118 security.

In order to control the amount of power that an EV may draw from a Charging Station, some form of vehicle to grid communication is necessary. OCPP has been designed to support the ISO 15118 standard for communication between the EV and Charging Station (EVSE). However, it is anticipated that for the coming years, the majority of EVs will only support the control pilot PWM signal IEC61851, so care has been taken to support smart charging with this as well.

NOTE A mapping of the ISO 15118 and OCPP terminology is provided in ISO 15118 and OCPP terminology mapping and abbreviations used in ISO 15118 are listed in ISO 15118 Abbreviations.

2. ISO 15118 Certificates

2.1. ISO 15118 Certificate structure

The ISO 15118 standard provides a Plug & Charge mechanism. This is an identification and authorization mode where the customer just has to plug his electric vehicle into the EVSE and all aspects of authentication, authorization, load control and billing are automatically taken care of without the need for further user interaction. This is facilitated by the application of digital signatures and exchange of X.509 certificates bound to a Public Key Infrastructures (PKI) model.

The PKI structure defined by ISO 15118 is shown in the figure below. In general, four PKIs need to be in place.

- PKI for the Charging Station Operator (CSO)
- PKI for the Certificate Provisioning Service (CPS)
- PKI for the Mobility Operator (MO)
- PKI for the car manufacturer (OEM)

The trust anchor (root CA) for the CSO and CPS is the so-called V2G Root CA. On the other hand, it is up to the respective OEM and MO to operate a Root CA of their own or derive their certificates from a V2G Root CA (indicated by the dotted lines between V2G Root and MO Sub-CA 1 and OEM Sub-CA 1, respectively).

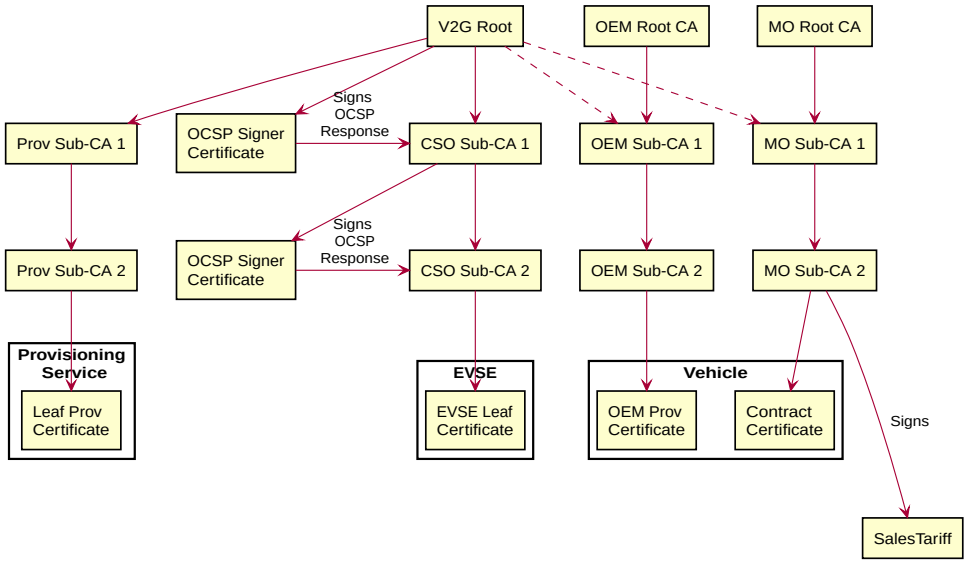

Figure 122. PKIs applied for Plug & Charge identification mode

If only one Sub-CA layer is used, i.e. a Sub-CA signed by a Root CA directly signs leaf certificates, the profile of Sub-CA 2 shall apply for that Sub-CA (Source: ISO15118-2)

OCPP needs to make sure that the necessary information can be exchanged between the EV, the Charging Station and a backend IT infrastructure to facilitate the contract provisioning. Contract provisioning is a process defined within ISO 15118 that describes how an EV can retrieve a valid contract certificate during a communication session in order to authenticate and authorize itself for the charging process.

Given the PKI structure in the figure above, OCPP must provide messages which are able to transmit the following certificates:

- **CPS certificate chain**
  Comprised of Prov Sub-CA 1, Prov Sub-CA 2 and leaf provisioning certificate. Sent with the CertificateInstallationRes and CertificateUpdateRes message.
- **MO certificate chain**
  Comprised of MO Sub-CA 1, MO Sub-CA 2 and contract certificate. Sent with the messages CertificateInstallationRes, CertificateUpdateReq, and CertificateUpdateRes.
- **OEM provisioning certificate**
  Sent with the CertificateInstallationReq message.

Furthermore, some ISO 15118 messages require digital XML-based signatures. Those signatures need to be validated by the receiving party by using the corresponding certificate chain and verifying the chain of signatures all the way up to the respective trust anchor (V2G root, MO root or OEM root). Table 13 on page 45 of ISO15118-2 provides an overview of applied XML-based

signatures in ISO 15118. As you can see in there, the Charging Station (EVSE is part of a Charging Station) needs to verify the signature of the following messages.

- **AuthorizationReq**
  Certificate chain needed to verify signature is provided with PaymentDetailsReq.
- **MeteringReceiptReq**
  Certificate chain needed to verify signature is provided with PaymentDetailsReq.
- **CertificateUpdateReq**
  Certificate chain needed to verify signature is provided with this message.

The signature verification as well as the check of the validity of each certificate provided by the EV can be done offline. These three messages are signed with the private key belonging to the public key of the contract certificate that is installed in the EV. The CSO needs to make sure that the corresponding MO root CA certificate (MO trust anchor) is installed on the Charging Station to enable signature verification offline (the chain of contract certificates and sub-CA certificates is already fulfilled by the EV in the PaymentDetailsReq message so only the MO root CA is required).

The PaymentDetailsReq message is sent before the AuthorizationReq and MeteringReceiptReq message. Therefore, the Charging Station must temporarily save the certificate chain provided with the PaymentDetailsReq message as long as the current transaction is active in order to be able to verify the signature created by the EV. After the transaction has been terminated, the temporarily saved certificate chain must be deleted on the Charging Station side.
Please note that the Charging Station only needs to check the contract certificate upon the receipt of the PaymentDetailsReq message *from* the EV which delivers the ContractSignatureCertChain, containing the contract certificate and possible sub-CA certificates, excluding the root CA certificate. *However*, it does not need to check the contract certificate upon installation or update of the contract certificate, upon delivery *to* the EV.

On the contrary, the signature provided with the **CertificateInstallationReq** needs to be verified by a so-called secondary actor, a market stakeholder communicating with the CSO backend. This means that OCPP needs to provide means for transmitting the complete CertificateInstallationReq message.

The CertificateUpdateRes and CertificateInstallationRes need to be sent from the CSO backend to the charging station as Base64 encoded binary data. The Charging Station removes the Base64 encoding and sends it to the EV as a binary EXI message.

Finally, the Charging Station certificate (labelled as EVSE Leaf Certificate in figure 1) together with its private key is used to establish a secure connection between EV and EVSE via TLS. According to ISO 15118, this certificate should be valid for only 2 to 3 months. To install or update the Charging Station certificate, please refer to Certificate installation Charging Station.

While the Charging Station can verify the signature and validity period of each certificate in the MO contract certificate chain offline, there are two things which the Charging Station cannot verify offline:

1. **The authorization status of the EMAID**
The EMAID is a unique identifier issued by the MO together with the contract certificate. Therefore, only the MO can provide information on whether the user is authorized for charging based on this EMAID or not. The Charging Station needs to forward the EMAID to the CSO after having checked that the signature of each certificate in the contract certificate chain is valid. This order of steps is necessary because the contract certificate protects the EMAID against manipulation by means of the digital signature of its issuer. The Charging Station could also work with a white list of EMAIDs cached locally. However, white lists need to be frequently updated to ensure that the authorization information used is not outdated.
2. **The revocation status of each certificate**
Reasons for revoking a certificate are e.g. that the private key belonging to the public key of a certificate has been corrupted or that the algorithm used to create a signature is not considered to be secure anymore. Revocation status is checked using an OCSP responder whose address is given as an attribute value of an X.509 certificate.

2.2. Using ISO 15118 Certificates in OCPP

From an OCPP perspective, based on the above paragraph, the Charging Station needs to have one or more of each of the following certificate types:

Type	Description
V2GChargingStation Certificate	Certificate of the Charging Station. In 15118 this is called the *SECC Certificate* (or *EVSE Leaf Certificate*). This certificate is used during the set-up of the TLS connection between the Charging Station and the EV.
V2GRootCertificate	Certificate of the V2G Root. The V2G Charging Station Certificate MUST BE derived from this root.
MORootCertificate	Certificate from an eMobility Service provider. To support PnC charging with contracts from service providers that not derived their certificates from the V2G root.

NOTE	The V2G Charging Station Certificate might be the same as the certificate used for securing the connection between the Charging Station and the CSMS. For this to work, this certificate MUST BE to be derived from a V2G Root.

A Contract Certificate can be derived from a V2G root, or an eMobility root. This means the Charging Station needs to be in possession of the corresponding root certificate to be able to authenticate the driver by means of the Contract Certificate and the associated certificate chain.

NOTE	When a Charging Station is online this does not have to be the case, because it can send an AuthorizeRequest message with the Contract Certificate to be validated by the CSMS.

The V2G Charging Station Certificate needs to be derived from a V2G root. If this root is not known by the EV, no connection via 15118 is possible, so charging controlled by 15118 is NOT possible. In the event a Charging Station needs to support more than one V2G root, multiple V2G Charging Station Certificates are needed.

2.3. 15118 communication set-up

At the beginning of a 15118 communication session the EV will initiate a TLS Connection. In this request, the car presents its known V2G root certificates.

During the TLS handshake, the EVCC can request the OCSP status of the Charging Station and intermediate certificates using OCSP stapling as defined in IETF RFC 6961. The Charging Station can retrieve this information by sending a GetCertificateStatusRequest to the CSMS, see use case M06 - Get Charging Station Certificate status.

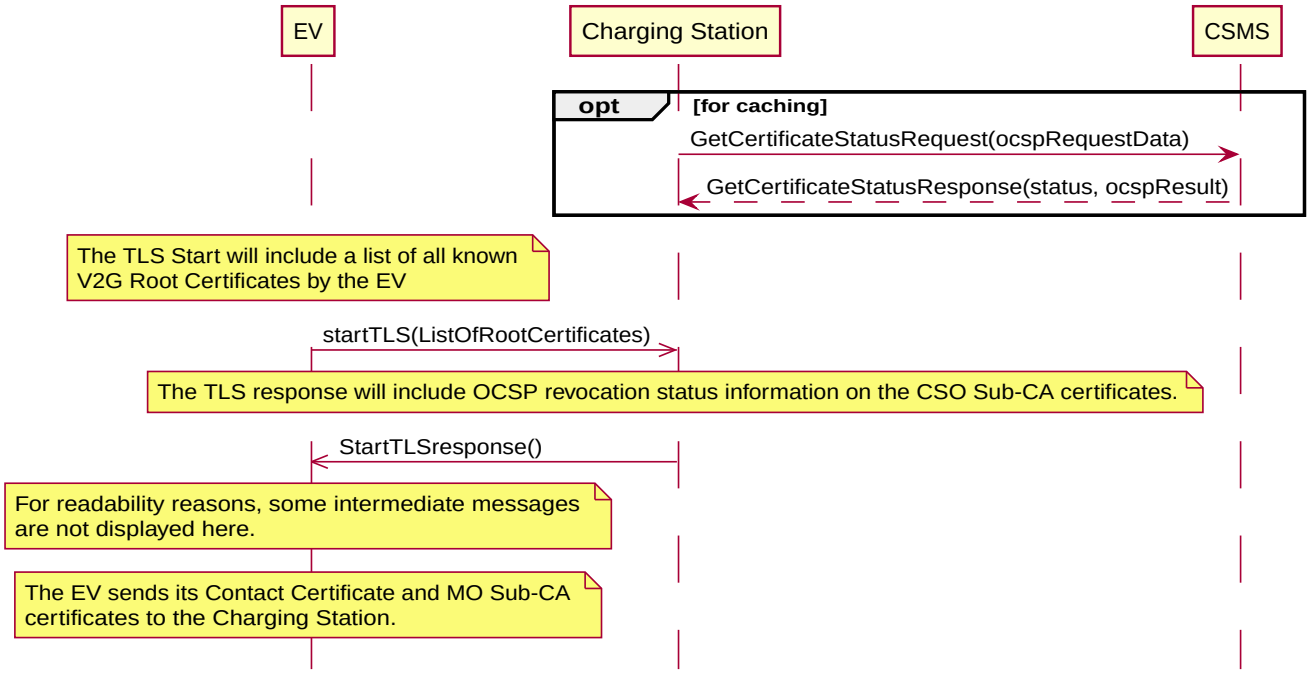

Figure 123. Communication set-up

2.4. Certificate - Use Case mapping

The following table contains the use cases that can be used to manage the certificates needed for ISO 15118 charging from OCPP:

Table 200. Certificates relevant for 15118

Certificate	Used for	Use Case	Remark
ChargingStationCertificate	Charging Station - CSMS connection	A02 and A03	Used for OCPP security in general. Certificate chain must also be available and can be retrieved by the Charging Station when installing the certificate.
CPS Certificate Chain	Plug & Charge authentication	M03, M04 and M05	
EVContractCertificate	Plug & Charge authentication	M01 and M02	Shorter life time certificate (for plug & charge)
MORootCertificate	Plug & Charge authentication	M03, M04 and M05	

Certificate	Used for	Use Case	Remark
MO Certificate Chain	Plug & Charge authentication	N.a.	It is only necessary to install MO root certificate for Plug & Charge authentication, other intermediate certificates are offered by the EV
OEMProvisioningCertificate	Installing Certificates in the EV	M01 and M02	Long life time installed in EV by OEM
V2GChargingStationCertificate	EV - Charging Station TLS connection	A02 and A03	Certificate chain must also be available and can be retrieved by the Charging Station when installing the certificate.
V2GRootCertificate	EV - Charging Station TLS connection	M03, M04 and M05	It is only necessary to install a V2G root certificate for Plug & Charge authentication.
V2GIntermediateCertificate	Plug & Charge authentication	A02, A03, M03 and M04	Intermediate certificates between the *V2GChargingStationCertificate* and *V2GRootCertificate*. May be used during TLS setup between EV and Charging Station.

3. Use cases from ISO 15118 relevant for OCPP

See ISO15118-1 page 17 for a list of all elementary use cases. The **bold** indicated use case component are identified as of influence of the OCPP communication following ISO15118-1.

Table 201. 15118 use cases relevant for OCPP (Source original table: ISO15118-1)

No.	Use case element name / grouping
A1	Begin of charging process with forced High Level Communication
A2	Begin of charging process with concurrent IEC61851-1 and High Level Communication
B1	**EV/Charging Station communication setup**
C1	**Certificate update**
C2	**Certificate installation**
D1	Authorization using Contract Certificates performed at the EVSE
D2	**Authorization using Contract Certificates performed with help of SA**
D3	Authorization at EVSE using external credentials performed at the EVSE
D4	**Authorization at EVSE using external credentials performed with help of SA**
E1	**AC charging with load leveling 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 leveling based on High Level Communication**
E5	Resume to Authorized Charge Schedule
F0	Charging loop
F1	Charging loop with metering information exchange
F2	**Charging loop with interrupt from the Charging Station**
F3	**Charging loop with interrupt from the EV or user**
F4	Reactive power compensation
F5	**Vehicle to grid support**
G1	Value added services
G2	Charging details
H1	**End of charging process**

NOTE Not all 15118 related OCPP use cases are described in *this* functional block. This functional block describes installing and updating certificates in the EV and CA certificate handling (also for non 15118 related purposes). Please refer to ISO 15118 Authorization for the authorization related use cases. The Smart Charging related use cases are described in the chapter Smart Charging.

4. Use cases & Requirements

M01 - Certificate installation EV

Table 202. M01 - Certificate installation

No.	Type	Description
1	**Name**	Certificate Installation
2	**ID**	M01
	Functional block	M. ISO 15118 Certificate Management
	Reference	ISO15118-1 C2
3	**Objectives**	To install a new certificate from the CSMS in the EV.
4	**Description**	The EV initiates installing a new certificate. The Charging Station forwards the request for a new certificate to the CSMS. See also ISO15118-1, use case Description C2, page 22.
	Actors	EV, Charging Station, CSMS
	Scenario description	**15118**: See ISO15118-1, use case Description C2, Scenario Description, first 3 bullets, page 22. **OCPP**: - The Charging Station sends Get15118EVCertificateRequest message **with *action* = `Install`** to the CSMS. - The CSMS responds with Get15118EVCertificateResponse to the Charging Station.
	Alternative scenario's	n/a
5	**Prerequisites**	See ISO15118-1, use case Prerequisites C2, page 22. - CSMS should be able to communicate with the contract certificate pool
6	**Postcondition(s)**	See ISO15118-1, use case End conditions C2, page 23.

Figure 124. Certificate Installation

7	**Error handling**	In case the CSMS is not able to respond within the specified time, the Charging Station SHALL indicate failure to the EV.
8	**Remark(s)**	The message timeout in ISO15118-2 for CertificateInstallationReq is 5 seconds. There may be alternative communication paths for doing a certificate installation. However, these are outside the scope of this standard.

Source: ISO15118-1

M01 - Certificate installation - Requirements

Table 203. M01 - Requirements

ID	Precondition	Requirement definition	Note
M01.FR.01	Upon receiving a 15118 CertificateInstallationReq	The Charging Station SHALL forward the request to the CSMS using the Get15118EVCertificateRequest message **with *action* = `Install`**.	The CSMS is responsible for forwarding it to the 15118 contract certificate pool.

M02 - Certificate Update EV

Table 204. M02 - Certificate Update

No.	Type	Description
1	**Name**	Certificate Update
2	**ID**	M02
	Functional block	M. ISO 15118 Certificate Management
	Reference	ISO15118-1 C1
3	**Objectives**	See ISO15118-1, use case Objective C1, page 20.
4	**Description**	See ISO15118-1, use case Description C1, page 21 up to and including the third "NOTE".
	Actors	EV, Charging Station
	Scenario description	**15118**: See ISO15118-1, use case Objective C1, Scenario Description, first 3 bullets, page 21. **OCPP**: - The Charging Station sends a Get15118EVCertificateRequest message **with *action* = `Update`** to the CSMS. - The CSMS responds with Get15118EVCertificateResponse to the Charging Station. **15118**: See ISO15118-1, use case Description C1, Scenario Description, last 2 bullets, page 21.
5	**Prerequisites**	- Communication between EV and EVSE SHALL be established successfully. - Online connection between Charging Station and CSMS SHALL be possible. - CSMS should be able to communicate with the contract certificate pool
6	**Postcondition(s)**	See ISO15118-1, use case Objective C1 and C2, page 20/22.

Figure 125. Certificate Update

7	**Error handling**	In case the CSMS is not able to respond within the specified time, the Charging Station SHALL indicate failure to the EV.
8	**Remark(s)**	See ISO15118-1, use case Requirements C1, trigger , page 21. The message timeout in ISO15118-2 for CertificateUpdateReq is 5 seconds.

Source: ISO15118-1

M02 - Certificate Update - Requirements

Table 205. M02 - Requirements

ID	Precondition	Requirement definition	Note
M02.FR.01		Upon receiving a CertificateUpdateReq the Charging Station SHALL forward the request to the CSMS using the Get15118EVCertificateRequest message **with *action* = `Update`**.	The CSMS is responsible for forwarding it to the 15118 contract certificate pool.

M03 - Retrieve list of available certificates from a Charging Station

Table 206. M03 - Retrieve list of available certificates from a Charging Station

No.	Type	Description
1	**Name**	Retrieve list of available certificates from a Charging Station
2	**ID**	M03
	Functional block	M. ISO 15118 Certificate Management
3	**Objective(s)**	To enable the CSMS to retrieve a list of available certificates from a Charging Station.
4	**Description**	To facilitate the management of the Charging Station's installed certificates, a method of retrieving the installed certificates is provided. The CSMS requests the Charging Station to send a list of installed certificates
	Actors	Charging Station, CSMS
	Scenario description	**1.** The CSMS requests the Charging Station to send a list of installed certificates by sending a GetInstalledCertificateIdsRequest **2.** The Charging Station responds with a GetInstalledCertificateIdsResponse
5	**Prerequisite(s)**	n/a
6	**Postcondition(s)**	The CSMS received a list of installed certificates

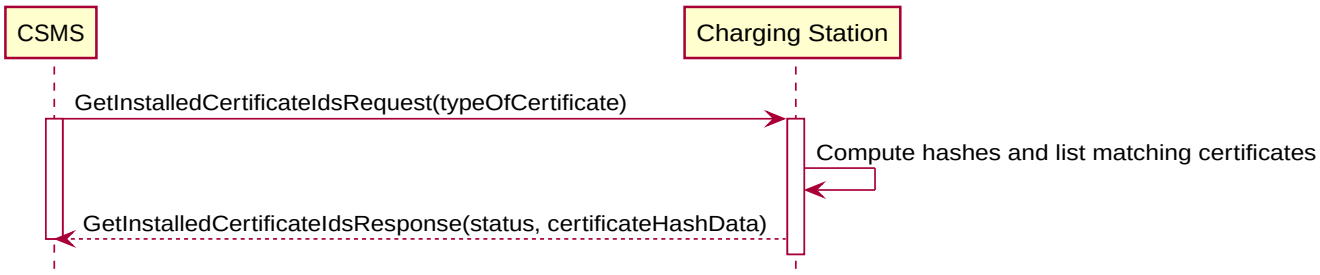

Figure 126. Retrieve list of available certificates from a Charging Station

7	**Error handling**	n/a
8	**Remark(s)**	For installing the (V2G) Charging Station Certificate, see use cases A02 - Update Charging Station Certificate by request of CSMS and A03 - Update Charging Station Certificate initiated by the Charging Station. The V2G certificate chain SHOULD not include the V2GRootCertificate. This SHOULD be installed using Use case M05 - Install CA certificate in a Charging Station.

M03 - Retrieve list of available certificates from a Charging Station - Requirements

Table 207. M03 - Requirements

ID	Precondition	Requirement definition
M03.FR.01	After receiving a GetInstalledCertificateIdsRequest	The Charging Station SHALL respond with a GetInstalledCertificateIdsResponse.
M03.FR.02	M03.FR.01 AND No certificate matching *typeOfCertificate* was found	The Charging Station SHALL indicate this by setting *status* in the GetInstalledCertificateIdsResponse to *NotFound*.
M03.FR.03	M03.FR.01 AND A certificate matching *typeOfCertificate* was found	The Charging Station SHALL indicate this by setting *status* in the GetInstalledCertificateIdsResponse to *Accepted*.
M03.FR.04	M03.FR.03	The Charging Station SHALL include the hash data for each matching installed certificate in the GetInstalledCertificateIdsResponse.

ID	Precondition	Requirement definition
M03.FR.05	When the Charging Station receives a GetInstalledCertificateIdsRequest with typeOfCertificate V2GCertificateChain	The Charging Station SHALL include the hash data for each installed certificate belonging to a V2G certificate chain. Sub CA certificates SHALL be placed as a childCertificate under the V2G Charging Station certificate.

M04 - Delete a specific certificate from a Charging Station

Table 208. M04 - Delete a specific certificate from a Charging Station

No.	Type	Description
1	**Name**	Delete a specific certificate from a Charging Station
2	**ID**	M04
	Functional block	M. ISO 15118 Certificate Management
3	**Objective(s)**	To enable the CSMS to request the Charging Station to delete an installed certificate.
4	**Description**	To facilitate the management of the Charging Station's installed certificates, a method of deleting an installed certificate is provided. The CSMS requests the Charging Station to delete a specific certificate.
	Actors	Charging Station, CSMS
	Scenario description	**1.** The CSMS requests the Charging Station to delete an installed certificate by sending a DeleteCertificateRequest. **2.** The Charging Station responds with a DeleteCertificateResponse.
5	**Prerequisite(s)**	n/a
6	**Postcondition(s)**	The requested certificate was deleted from the Charging Station.

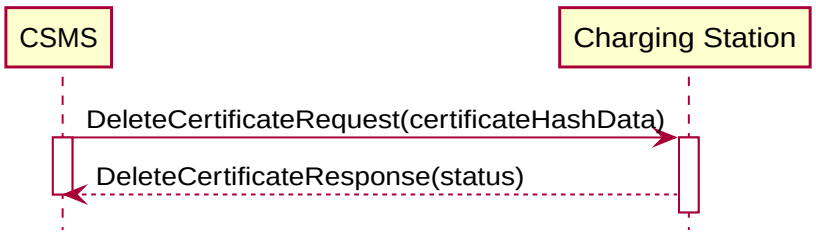

Figure 127. Delete Installed Certificate

7	**Error handling**	n/a
8	**Remark(s)**	For installing the (V2G) Charging Station Certificate, see use cases A02 - Update Charging Station Certificate by request of CSMS and A03 - Update Charging Station Certificate initiated by the Charging Station. The V2G certificate chain SHOULD not include the V2GRootCertificate. This SHOULD be installed using Use case M05 - Install CA certificate in a Charging Station. It is possible to delete the last (every) installed CSMSRootCertificates. When all CSMSRootCertificates are deleted, the Charging Station cannot validate CSMS Certificates, so it will not be able to connect to a CSMS. Before a CSMS would ever send a DeleteCertificateRequest that would delete the last/all CSMSRootCertificates the CSMS is ADVISED to make very sure that this is what is really wanted. It is possible to delete the last (every) installed ManufacturerRootCertificates, when all ManufacturerRootCertificates are deleted, no "Signed Firmware" can be installed in the Charging Station.

M04 - Delete a specific certificate from a Charging Station - Requirements

Table 209. M04 - Requirements

ID	Precondition	Requirement definition	Note
M04.FR.01	After receiving a DeleteCertificateRequest	The Charging Station SHALL respond with a DeleteCertificateResponse.	

ID	Precondition	Requirement definition	Note
M04.FR.02	M04.FR.01 AND The requested certificate was found	The Charging Station SHALL delete it, and indicate success by setting 'status' to 'Accepted' in the DeleteCertificateResponse.	
M04.FR.03	M04.FR.01 AND The deletion fails	The Charging Station SHALL indicate failure by setting 'status' to 'Failed' in the DeleteCertificateResponse.	
M04.FR.04	M04.FR.01 AND The requested certificate was not found	The Charging Station SHALL indicate failure by setting 'status' to 'NotFound' in the DeleteCertificateResponse.	
M04.FR.06		Deletion of the *Charging Station Certificate* SHALL NOT be possible via a DeleteCertificateRequest.	
M04.FR.07	When deleting a certificate	The CSMS SHALL use the *hashAlgorithm*, which was used to install the certificate.	When a new firmware is installed it is RECOMMENDED that the CSMS requests the certificate first using GetInstalledCertificateIdsRequest to be sure of the used *hashAlgorithm*.

M05 - Install CA certificate in a Charging Station

Table 210. M05 - Install CA certificate in a Charging Station

No.	Type	Description
1	**Name**	Install CA certificate in a Charging Station
2	**ID**	M05
	Functional block	M. ISO 15118 Certificate Management
3	**Objective(s)**	To facilitate the management of the Charging Station's installed certificates, a method to install a new CA certificate.
4	**Description**	The CSMS requests the Charging Station to install a new CSMS root certificate, Sub-CA certificate for an eMobility Operator, Manufacturer root, or a V2G root certificate.
	Actors	Charging Station, CSMS
	Scenario description	**1.** The CSMS requests the Charging Station to install a new certificate by sending an InstallCertificateRequest. **2.** The Charging Station responds with an InstallCertificateResponse.
5	**Prerequisite(s)**	n/a
6	**Postcondition(s)**	The new certificate was installed in the Charging Station trust store.

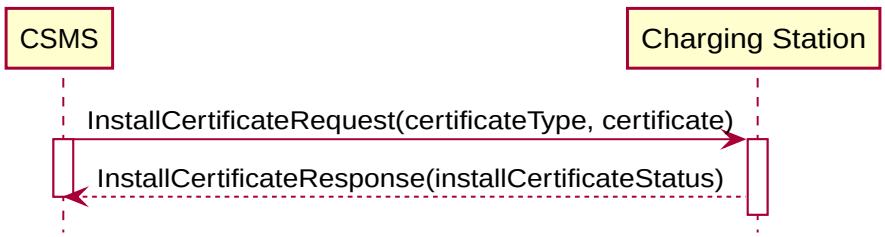

Figure 128. Install CA certificate in a Charging Station

7	**Error handling**	n/a

8	**Remark(s)**	Even though the messages CertificateSignedRequest (see use cases A02 - Update Charging Station Certificate by request of CSMS and A03 - Update Charging Station Certificate initiated by the Charging Station) and InstallCertificateRequest (use case M05) are both used to send certificates, their purposes are different. CertificateSignedRequest is used to return the the Charging Stations own public certificate and V2G certificate(s) signed by a Certificate Authority. InstallCertificateRequest is used to install Root certificates. For installing the (V2G) Charging Station Certificate, see use cases A02 - Update Charging Station Certificate by request of CSMS and A03 - Update Charging Station Certificate initiated by the Charging Station. The V2G certificate chain SHOULD not include the V2GRootCertificate. This SHOULD be installed using this use case. It is allowed to have multiple certificates of the same type installed.

M05 - Install CA certificate in a Charging Station - Requirements

Table 211. M05 - Requirements

ID	Precondition	Requirement definition
M05.FR.01	After receiving an InstallCertificateRequest	The Charging Station SHALL attempt to install the certificate and respond with an InstallCertificateResponse.
M05.FR.02	M05.FR.01 AND The installation was successful	The Charging Station SHALL indicate success by setting 'status' to 'Accepted' in the InstallCertificateResponse.
M05.FR.03	M05.FR.01 AND The installation failed	The Charging Station SHALL indicate failure by by setting 'status' to 'Failed' in the InstallCertificateResponse.
M05.FR.06	When a new certificate gets installed AND the CertificateEntries.maxLimit is going to be exceeded	The Charging Station SHALL respond with status *Rejected*.
M05.FR.07	M05.FR.01 AND The certificate is invalid.	The Charging Station SHALL indicate rejection by setting 'status' to 'Rejected' in the InstallCertificateResponse.
M05.FR.09	When `AdditionalRootCertificateCheck` is true	Only one certificate (plus a temporarily fallback certificate) of certificateType CSMSRootCertificate is allowed to be installed at a time.
M05.FR.10	When `AdditionalRootCertificateCheck` is true AND installing a new certificate of certificateType CSMSRootCertificate	The new CSMS Root certificate SHALL replace the old CSMS Root certificate AND the new Root Certificate MUST be signed by the old Root Certificate it is replacing
M05.FR.11	M05.FR.10 AND the new CSMS Root certificate is NOT signed by the old CSMS Root certificate	The Charging Station SHALL NOT install the new CSMS Root Certificate and respond with status *Rejected*.
M05.FR.12	M05.FR.10 AND the new CSMS Root certificate is signed by the old CSMS Root certificate	The Charging Station SHALL install the new CSMS Root Certificate AND temporarily keep the old CSMS Root certificate as a fallback certificate AND respond with status *Accepted*
M05.FR.13	M05.FR.12 AND the Charging Station successfully connected to the CSMS using the new CSMS Root certificate	The Charging Station SHALL remove the old CSMS Root (fallback) certificate.
M05.FR.14	M05.FR.12 AND The Charging Station is attempting to reconnect to the CSMS (NOT migrating to another CSMS with Use Case B10 - Migrate to new CSMS), but determines that the server certificate provided by the CSMS is invalid when using the new CSMS Root certificate to verify it	The Charging Station SHALL try to use the old CSMS Root (fallback) certificate to verify the server certificate.

ID	Precondition	Requirement definition
M05.FR.15	M05.FR.12 AND When the Charging Station is migrating to another CSMS with Use Case B10 - Migrate to new CSMS, but determines that the server certificate provided by the CSMS is invalid when using the new CSMS Root certificate to verify it	The Charging Station SHALL use the `NetworkProfileConnectionAttempts` mechanism as described at Use Case B10 - Migrate to new CSMS .
M05.FR.16	M05.FR.15 AND If after the number of attempts the connection fails AND If it goes back to the old NetworkConnectionProfile (*See B10.FR.03*)	The Charging Station SHALL use the old CSMS Root (fallback) certificate to verify the server certificate.

M06 - Get V2G Charging Station Certificate status

Table 212. M06 - Get V2G Charging Station Certificate status

No.	Type	Description
1	**Name**	Get V2G Charging Station Certificate status
2	**ID**	M06
	Functional block	M. ISO 15118 Certificate Management
3	**Objective(s)**	To enable a Charging Station to cache the OCSP certificate status needed for the TLS handshake between EV and Charging Station.
4	**Description**	When the cable gets plugged in and an ISO 15118 supported EV gets connected to the Charging Station, the EV requests the Charging Station to prove the validity of the (SubCA) certificates by an OCSPResponse. A request needs to be sent per SubCA. Because the timeout constraint in ISO 15118 is too strict to make the call to an external server, OCPP requires to cache the OCSP certificate status of the certificates beforehand. The Charging Station needs to refresh the cached OCSP data once a week..
	Actors	Charging Station, CSMS
	Scenario description	**1.** The Charging Station requests the CSMS to provide OCSP certificate status by sending a GetCertificateStatusRequest. **2.** The CSMS responds with a GetCertificateStatusResponse.
5	**Prerequisite(s)**	n/a
6	**Postcondition(s)**	**Successful postcondition:** The Charging Station received the OCSP certificate status for the requested certificate **Failure postcondition:** The retrieval of the OCSP certificate status by the CSMS failed

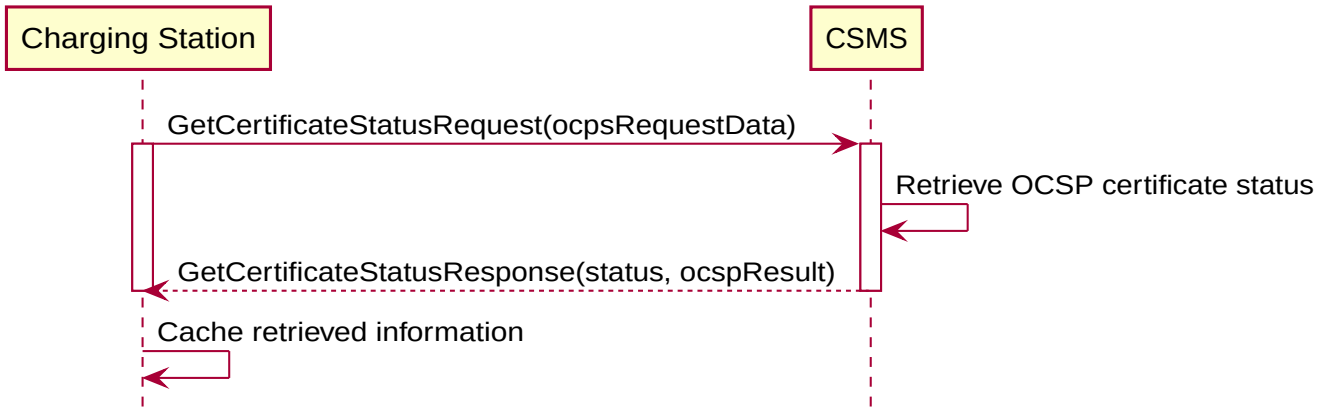

Figure 129. Get V2G Charging Station Certificate status

7	**Error handling**	n/a

8	**Remark(s)**	The status indicator in the GetCertificateStatusResponse indicates whether or not the CSMS was successful in retrieving the certificate status. it does NOT indicate the validity of the certificate. For installing the (V2G) Charging Station Certificate, see use cases A02 - Update Charging Station Certificate by request of CSMS and A03 - Update Charging Station Certificate initiated by the Charging Station. The V2G certificate chain SHOULD not include the V2GRootCertificate. This SHOULD be installed using Use case M05 - Install CA certificate in a Charging Station. OCPP allows for only one certificate per GetCertificateStatusRequest. Because when multiple answers on a GetCertificateStatusRequest are to be expected, it makes handling the request and status more complex. So a GetCertificateStatusRequest needs to be sent per SubCA. *responderURL* is required in OCPP, while it is optional in ISO 15118. Without a *responderURL* in a certificate it cannot work, so a *responderURL* is required for any certificate for which a GetCertificateStatusRequest can be expected.

M06 - Get V2G Charging Station Certificate status - Requirements

Table 213. M06 - Requirements

ID	Precondition	Requirement definition
M06.FR.01	After receiving a GetCertificateStatusRequest	The CSMS SHALL respond with a GetCertificateStatusResponse.
M06.FR.02	M06.FR.01 AND The CSMS was successful in retrieving the OCSP certificate status	The CSMS SHALL indicate success by setting 'status' to 'Accepted' in the GetCertificateStatusResponse.
M06.FR.03	M06.FR.02	The CSMS SHALL include the OCSP response data in the OCSPResult field in the GetCertificateStatusResponse.
M06.FR.04	M06.FR.01 AND The CSMS was not successful in retrieving the OCSP certificate status	The CSMS SHALL indicate it was not successful by setting 'status' to 'Rejected' in the GetCertificateStatusResponse.
M06.FR.06		The Charging Station SHALL request and cache the OCSP status for its V2G certificates.
M06.FR.07		After the Charging Station Certificate has been updated, The Charging Station SHALL refresh the cached OCSP data by sending a GetCertificateStatusRequest for the new certificate, and also for the intermediate certificates.
M06.FR.08		The CSMS SHALL format the response data according to OCSPResponse as defined in IETF RFC 6960, formatted according to ASN.1 [X.680].
M06.FR.09		The OCSPResponse data SHALL be DER encoded.
M06.FR.10		The Charging Station SHALL refresh the cached OCSP data at least once a week.