Requirements EVSE CHECK for PnC with ISO15118-2

Requirements in compliancy with V2G-PKI and PnC Ecosystem

HUBJECT

Authors Arne Schlowak, Ivan Safronov
Contacts Arne.Schlowak@hubject.com, Ivan.Safronov@hubject.com

Date 24 July 2024

Versioning

Version	Datum	Autor	Comment
V1.0	06.11.2019	Jonel Timbergen	*Initial creation of Document*
V1.1	01.08.2020	Tim Kleeberg	*Editing some typos*
V1.2	15.09.2020	Jonel Timbergen	Added requirements for Hardware Security Modules in Chapter 5
V1.3	10.10.2020	Jonel Timbergen	Textual updates OCA application note information
V1.4	15.04.2021	Tim Kleeberg	Deleting section about Key-Pair generation in other locations than EVSE/SECC
V1.5	24.01.2022	Tim Kleeberg	Changing the Title to Requirements for EVSEs and focusing on PKI and Ecosystem requirements only for EVSEs. Adding OCPP OCA Requirement Deleting old UseCases from OCPP 2.0
V1.6	03.02.2022	Tim Kleeberg	Adding requirements for configurable Distinguished Name in EVSE Leaf CSR
V1.7	15.02.2022	Tim Kleeberg	Textual editing 4.1 edited. Deleted Key sizes & Cryptographic module standards and controls References Added PnC custom OCPP Configuration Key Names & Values Added required deviation from OCPP Message Get15118EVCertificate Added description of SECCID Defining what V2G Certificates are seen as trustworthy
V1.8	15.08.2022	Tim Kleeberg	Changing OCPP configuration key SeccLeafSubjectCommonName (2.4.1)
V1.9	21.09.2022	Tim Kleeberg	Changing 2.8 to informative Rephrasing and ascertainment of 1. Introduction Adding in 2.8.1 information about the OCSP request for the complete contract chain, not just for the contract leaf. Clarifications in chapter 2.9 Change in checksums for SECCIDs examples in 0

V2.0	26.06.2023	Arne Schlowak	Changing 4.3 to informative because the CPMS is in charge. Clarifications in chapter 4.5 on how to handle certificate status via OCSP for the EVSE leaf certificate
V2.1	04.07.2023	Arne Schlowak	Clarification in section 2.8 and addition of a authorize.req example message Clarification in section 4.1 and 4.2.
V3.0	29.02.2024	Arne Schlowak	Changing requirements into a more formal requirements format based on the “Requirements EVSE CHECK for PnC based on OCPP 2.0.1” document (v2.1).
V3.1	27.06.2024	Arne Schlowak	Added: HUB-25-006, HUB-25-007, HUB-31-004 Clarified: HUB-22-001, HUB-23-001, HUB-25-002, HUB-25-005, HUB-281-006, 2.9 chapter clarified
V4	24.07.2024	Ivan Safronov	“Requirements EVSE CHECK for PnC based on OCPP 1.6” and “Requirements EVSE CHECK for PnC based on OCPP 2.0.1” are merged in one document “Requirements EVSE CHECK for PnC with ISO15118-2”. 2.8.3 chapter added 3.2 chapter deleted 3.4 chapter deleted requirements moved to 3.1 + References updated Added: HUB-24-002, HUB-24-003, HUB-242-001, HUB-25-008, HUB-281-008, HUB-281-009, HUB-283-001, HUB-283-002, HUB-283-003, HUB-283-004. Renamed: HUB-31-005 from HUB-34-001, HUB-31-006 from HUB-34-002, HUB-31-007 from HUB-34-003. Deleted duplicated: HUB-281-007, HUB-33-002. HUB-24-001 renamed to HUB-241-001 HUB-32-001 replaced with HUB-31-005 HUB-32-002 replaced with HUB-31-006 HUB-32-003 replaced with HUB-31-007 Clarified: HUB-23-004, HUB-23-005, HUB-25-003, HUB-281-001, HUB-281-002, HUB-281-003, HUB-281-004, HUB-281-005, HUB-281-006, HUB-282-001, HUB-282-003, HUB-211-001, HUB-211-002, HUB-212-001.

Index

List of Abbreviations

Abbreviation	Description
CA	Certificate authority
CCP	Contract Certificate Pool
CN	Common Name
CPMS	Charge Point Management System
CPO	Charge Point Operator
CPS	Certificate Provisioning Service
CRL	Certificate Revocation List
CSMS	Charging Station Management System
CSR	Certificate Signing Request
DHPublicKey	Diffie-Hellman Public Key
DN	Distinguished Name
EIM	External Identification Means
EMAID	E-Mobility Account Identifier
EVSE	Electric vehicle supply equipment (also Charge Point [CP] or Charging Station [CS)]
EVSEID	Electric Vehicle Supply Equipment ID
HSM	Hardware Secure Module
MO	Mobility Operator
OCA	Open Charge Alliance
OCPP	Open Charge Point Protocol (published by OCA)
OCSP	Online Certificate Status Protocol
PCP	Provisioning Certificate Pool
PCID	Provisioning Certificate Identifier

PKI	Public Key Infrastructure
PnC	Plug&Charge
QA	Quality Assurance
RCP	Root Certificate Pool
SECC	Supply Equipment Communication Controller
SECCID	Identifier of SECC used in the SECC Leaf Certificate's CN
SSD	Solid State Drive
TPM	Trusted Platform Module
V2G	Vehicle To Grid
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e.V

1 Introduction

This document serves as a basis for understanding what security and processual measures need to be considered on EVSE side to enable a seamless Plug&Charge experience.

The listed requirements are divided into the following categories:

- Security
- Processual
- Informative

For a successful “EVSE CHECK for PnC with ISO 15118-2”, you must comply with the respective status in all chapters marked with "security" and "processual".

The handling, implementation or realization of these stipulated requirements need to be documented and explicitly explained by the EVSE manufacturer.

Requirements marked with "informative" shall be acknowledged by the client to ensure interoperability and best practices in the field and deepen the knowledge.

Explanations on how the requirements are handled shall be included in a written “compliance report”. The introductory chapter of the compliance report should contain the following:

- Manufacturer company name
- Company address
- Registration number
- Date of submission of the report
- Product information
  - Manufacturer
  - Product Name
  - Technical Specification (max voltage, max current, number of charge connectors, etc.)
  - Firmware Version to be used for the certification process

2 Requirements for hardware and software in the EVSE/SECC

2.1 Protection of private keys of the SECC leaf certificates (security)

ID	Requirement Definition
HUB-21-001	All private keys shall be protected against unauthorized third-party access.
HUB-21-002	All private keys shall be encrypted with a secure and non-deprecated algorithm when stored in persistent (long-term) memory, including but not limited to SSD, flash drives, memory cards, and other non-volatile storage devices.
HUB-21-003	Decrypted private keys shall never be stored in persistent memory.
HUB-21-004	Private keys for the SECC leaf certificates shall never leave the embedded device on which they are generated.
OCPP 2.0.1 A02.FR.05	The private keys shall not be readable via OCPP or any other (remote) communication connection
HUB-21-005	TPM (Trusted Platform Module), HSM (Hardware Security Module) or similar technologies may be utilized to secure the private keys.
HUB-21-006	If encryption via software is used, the passphrase to secure the private keys shall be generated uniquely for each charger and shall not be predictable.

2.2 Initial trust anchor installation (processual)

ID	Requirement Definition
HUB-22-001	It is recommended to install Hubject's V2G productive root certificates during the manufacturing process.
HUB-22-002	The EVSE shall be capable of receiving new Root Certificates (e.g. V2G Root and MO Root) during operation.
HUB-22-003	The EVSE may install an additional root to enable a secure OCPP connection to the CPMS before it is used in the field for the first time.

2.3 Creation of an EVSE Leaf Certificate Sign Request (security)

ID	Requirement Definition
HUB-23-001	The EVSE needs to create a CSR conform to RFC2986 PKCS#10 format to request an EVSE-Leaf-Cert via the CPMS at the V2G PKI.
HUB-23-002	This CSR shall follow the Certificate Profile on Annex F of ISO 15118-2 respectively Hubject's V2G Certificate Policy.
HUB-23-003	The SECC Leaf Cert shall possess the SECCID as defined in ISO 15118-20 in its Common Name (CN) as well as the Organization (O) and Country (C) of the CPO. Independently, the Domain Component (DC) shall be "CPO". Note: The Common Name shall be set to the SECCID as defined in ISO 15118-20 since in ISO 15118-2 the content of the Common Name was not formally defined.
HUB-23-004	The EVSE shall allow the CPO to set the Common Name (CN), the Organization (O) and the Country (C) in the CSR of the SECC leaf certificate. For this purpose, the EVSE shall implement the OCPP Configuration Variables/Keys as described in section 2.4 Required Configuration Variables/Keys to enable PnC (security)
HUB-23-005	The EVSE may allow the CPO to set the EVSEIDs of the charge connector. For this purpose, the EVSE shall implement the OCPP Configuration Variables/Keys as described in section 2.4 Required Configuration Variables/Keys to enable PnC (security)

Example of an CSR:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBWzCCAQICAQAwcTETMBEGCgmSJomT8ixkARkWA0NQTzELMAkGA1UEBhMCREUxFTATBgNVBAoM
DEh1YmplY3QgR21iSDE2MDQGA1UEAwwtREVJQ0VTSFVCUkVRVUlSRU1FTlRTRVZTRUNIRUNLRk9S
SVNPMTUxMTgyUE5DMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEjF75a524CX06JJi5eRDBiuzh
udEp3nhPeF1JWVE59cxul+4nl8c6fYq8+g6owqXzQb/7ikgVsQORURQkn4QNXqAvMC0GCSqGSIb3
DQEJDjEgMB4wDAYDVR0TAQH/BAIwADAOBgNVHQ8BAf8EBAMCA4gwCgYIKoZIzj0EAwIDRwAwRAIg
JX82Utk6mAYL5YKIEtpYiz9COc104vu2WeU7I1d8l5kCIDN2ndFs7m6E0N9AWcbPWUqG5P2N/tuF
OkiSTG7ofyoG
-----END CERTIFICATE REQUEST-----
```

2.4 Required Configuration Variables/Keys to enable PnC (security)

To configure PnC capable EVSEs to comply with Hubject's requirements the following OCPP Configuration shall be implemented.

ID	Requirement Definition
HUB-24-002	The EVSE shall reject all requested changes of the below specified Configuration Variables/Keys with status equals to "rejected" if specifications of the Configuration Variables/Keys are not met.
HUB-24-003	If the optional Configuration Key "ConnectorEvseIds" or Configuration Variable "ISO15118EvseId" is implemented, the EVSE shall validate the minimum and maximum length of the EVSEID set by the CSMS in accordance with ISO 15118-2 (minimum length: 7, maximum length: 37). If the value is incorrect or no value is provided, the EVSEID shall be set to the default value "ZZ00000".

2.4.1 OCPP 1.6 Configuration Keys and Values (security)

ID	Requirement Definition
HUB-241-001	The EVSE shall implement the following additional OCPP Configuration keys.

Note: The following additional configuration keys give the CPO the possibility to alter the CSR for the SECC Leaf certificate in compliance with Hubject's certificate policy and to change the EVSEID of the charge connectors.

SeccLeafSubjectCommonName

Necessity	Required
Mutability	Read, Write (RW)
Type	string [7..64]
Description	Common Name(s) of the SECC (EVSE) leaf certificate(s). The CN shall be a SECCID. <SECCID> = <Country Code> <S> <EVSE Operator ID> <S> <ID Type> <S> <ControllerID> <S> <*Check Digit> Example: DEICES00003C4NABBB55787867564533096754347 6 Note: The Check Digit is optional and is not checked by Hubject's backend.

SeccLeafSubjectCountry

Necessity	Required
Mutability	Read, Write (RW)
Type	string [2]
Description	County of the SECC (EVSE) leaf certificate. Indicates in which country the CPO operates. Example: DE

SeccLeafSubjectOrganization

Necessity	Required
Mutability	Read, Write (RW)
Type	string [0..64]
Description	Organization of the SECC (EVSE) leaf certificate. Indicates which CPO operates this EVSE. Example: Hubject GmbH

ConnectorEvseIds

Necessity	Optional
Mutability	Read, Write (RW)
Type	string [7..1000]

Description	Comma separated EVSEIDs for OCPP connectors starting with connector 1 in one string. (concatenating multiple EVSEIDs is possible)
	
	Example (with different formatting):
	
	`“DE*ICE*EHUBIDFOROCPP1”`
	`“DEICEEidFORocppCONNECTOR1,DE*ICE*E*id*FORocpp*CONNECTOR*2”`
	`“DE*ICEEHUBIDFOROCPP1”`

2.4.2 Required OCPP 2.0.1 Configuration Variable Names and Values (security)

To configure PnC capable EVSEs to comply with Hubject's requirements the following OCPP Configuration Variable shall be implemented.

ID	Requirement Definition
HUB-242-001	The EVSE shall implement the following OCPP Configuration Variables defined by "OCPP 2.0.1 Part 2 – Specification edition 2 FINAL, 2022-12-15".

Note: The following variables give the CPO the possibility to alter the CSR for the SECC Leaf certificate in compliance with Hubject's certificate policy and to change the EVSEID of the charge connectors.

ISO15118SeccId

Necessity	Required
Mutability	Read, Write (RW)
Type	string [7..64]
ComponentName	ISO15118Ctrlr
Description	Common Name(s) of the SECC (EVSE) leaf certificate(s). The CN shall be a SECCID. <SECCID> = <Country Code> <S> <EVSE Operator ID> <S> <ID Type> <S> <ControllerID> <S> <*Check Digit> Example: DEICES00003C4NABBB5578786756453309675434 76 Note: The Check Digit is optional and is not checked by Hubject's backend.

ISO15118CountryName

Necessity	Required
Mutability	Read, Write (RW)
Type	string [2]
ComponentName	ISO15118Ctrlr
Description	County of the SECC (EVSE) leaf certificate. Indicates in which country the CPO operates. Example: “DE”

ISO15118OrganizationName

Necessity	Required
Mutability	Read, Write (RW)
Type	string [0..64]
ComponentName	ISO15118Ctrlr
Description	Organization of the SECC (EVSE) leaf certificate. Indicates which CPO operates this EVSE. Example: “Hubject GmbH”

ISO15118EvseId

Necessity	Optional
Mutability	Read, Write (RW)
Type	string [7..1000]
ComponentName	ISO15118Ctrlr
Description	The name of the EVSE in the string format as required by ISO 15118 and IEC 63119-2. Example: "DE*ICE*E*1234567890*1"

2.5 Handling of SECC Leaf Certificate (processual)

ID	Requirement Definition
HUB-25-001	The EVSE shall store an SECC Leaf Certificate and its corresponding chain to establish a secure communication between charger and vehicle.
OCPP 2.0.1 A02	The EVSE shall have the ability to create a new keypair and certificate signing request (CSR) triggered by the CSMS as specified in Use Case OCPP 2.0.1 A02.
OCPP 2.0.1 A03	The EVSE shall have the ability to create a new keypair and certificate signing request (CSR) automatically as specified in Use Case OCPP 2.0.1 A03.
HUB-25-002	The EVSE shall only replace the old SECC Leaf Certificate once a new SECC Leaf Certificate from the same V2G root has been delivered and is validated successfully.
HUB-25-003	The EVSE shall not store more than one SECC Leaf Certificate from the same V2G root and corresponding private key at the same time.
OCPP 2.0.1 A03.FR.06	The Charging Station SHALL verify the validity of the signed certificate in the OCPP CertificateSigned Request message, checking at least the period when the certificate is valid, the properties in Certificate Properties, and that it is part of the Charging Station Operator certificate hierarchy as described in Certificate Hierarchy.
HUB-25-004	If the CPMS sends an SECC leaf certificate chain including the V2G root certificate, the SECC shall ignore the V2G Root Certificate sent with the chain.
HUB-25-005	The EVSE shall validate the SECC Leaf certificate chain before installation against the V2G Root Certificate and reject installation if no trusted V2G Root Certificate can be found.
HUB-25-006	The EVSE may store multiple SECC Leaf Certificate chain signed from different V2G roots in its SECC. Note: This is relevant for multi PKI uses cases.
HUB-25-007	To increase interoperability, it is recommended to use the latest received SECC Leaf Certificate chain for V2G TLS communication if the EV doesn't present the "trusted_ca_keys" extension and EVSE has more than one SECC Leaf Certificate chain installed. Note: The "trusted_ca_keys" extension is mandatory in the "client hello" message of the EV but is sometimes not specified.

HUB-25-008	If multiple SECC Leaf certificate chains are needed in the EVSE, another SignCertificate request may be automatically send after receiving the first SignedCertificate response. Note: One SECC Leaf Certificate chain may be used for each charge connector.

2.6 How to handle a OCPP CertificateSigned Request (informative)

The OCPP CertificateSigned Request will include the signed PEM encoded X.509 certificates of the CPO chain in the “certificateChain” field.

SECC Leaf certificate
CPO Sub-CA 2
CPO Sub-CA 1

The certificate chain will include the relevant Sub CA certificate and must start from the SECC Leaf Certificate. This leads to the following schematical structure of the “certificateChain”:

Example of a CertificateSigned.req for OCPP 1.6:


```
[
 2,
 "123456789",
 "DataTransfer",
 {
  "vendorId": "org.openchargealliance.iso15118pnc",
  "messageId": "CertificateSigned",
  "data": "{\"certificateChain\": \"-----BEGIN CERTIFICATE-----\\nMIICOjCCAeCgAwIBAgIQYVC3KfGq0abwLMa
   FjIDG+DAKBggqhkjOPQQDAjBEMQsw\\nCQYDVQQGEwJERTEVMBMGA1UEChMMSHViamVjdCBHbWJIMR4wHAYDVQQDExVDUE8g\\
   nU3ViMiBDQSBRQSBHMS4yLjIwHhcNMjQwNzI0MTQwOTM1WhcNMjQxMDI0MTQwOTM1\\nWjBxMQswCQYDVQQGEwJERTEVMBMGA1
   UEChMMSHViamVjdCBHbWJIMTYwNAYDVQQD\\nEy1ERUlDRVNIVUJSRVFVSVJFTUVOVFNFVlNFQ0hFQ0tGT1JJU08xNTExODJQT
   kMx\\nEzARBgoJkiaJk/IsZAEZFgNDUE8wWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASM\\nXvlrnbgJfTokmLl5EMGK7OG50
   SneeE94XUlZUTn1zG6X7ieXxzp9irz6DqjCpfNB\\nv/uKSBWxA5FRFCSfhA1eo4GGMIGDMAwGA1UdEwEB/wQCMAAwEQYDVR0O
   BAoECE+u\\nX7KaVUZ3MBMGA1UdIwQMMAqACEeBskEROhG/MDsGCCsGAQUFBwEBBC8wLTArBggr\\nBgEFBQcwAYYfaHR0cDov
   L29jc3AtcWEuaHViamVjdC5jb206ODA4MDAOBgNVHQ8B\\nAf8EBAMCA4gwCgYIKoZIzj0EAwIDSAAwRQIhAJzSjcMgpv8pKYk
   /oJB6g+5SLvv/\\nfIajt/ybR6eOYg+xAiBuEoerEeQRFGsI0em02S9ylvsESrAvMVxIhfVwvQiPGA==\\n-----END CERTIF
   ICATE-----\\n-----BEGIN CERTIFICATE-----\\nMIICFTCCAbqgAwIBAgIQcowq33e0GXvgnfM3GEiJQjAKBggqhkjOPQQ
   DAjBCMQsw\\nCQYDVQQGEwJERTEVMBMGA1UEChMMSHViamVjdCBHbWJIMRwwGgYDVQQDExNDUE8g\\nU3ViMSBDQSBRQSBHMS4
   yMB4XDTI0MDIyODEzNTg0NVoXDTI2MDQwNjEyNTg0NVow\\nRDELMAkGA1UEBhMCREUxFTATBgNVBAoTDEh1YmplY3QgR21iSD
   EeMBwGA1UEAxMV\\nQ1BPIFN1YjIgQ0EgUUEgRzEuMi4yMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE\\nPHrw6dEPSV8YRp
   H2K3tkhS1Xn5AVRxZUlpPmuOFfPXkNciLe7O78Yasxd2Nmx02c\\nXwa5UIg7HqWckwfHMLb0saOBjzCBjDASBgNVHRMBAf8EC
   DAGAQH/AgEAMBEGA1Ud\\nDgQKBAhHgbJBEToRvzATBgNVHSMEDDAKgAhAFPvw56ljrDA+BggrBgEFBQcBAQQy\\nMDAwLgYIK
   wYBBQUHMAGGImh0dHA6Ly91cy5vY3NwLXFhLmh1YmplY3QuY29tOjgw\\nODAwDgYDVR0PAQH/BAQDAgEGMAoGCCqGSM49BAMC
   A0kAMEYCIQDmnpai8pt6yGCr\\nJzGdiybuSblVGbhBWmeyqP42h7C7YwIhAPnqxXMWbmnp1e81x0EK3JOLFbSNBL3a\\nA8w9
   gmnaKX54\\n-----END CERTIFICATE-----\\n-----BEGIN CERTIFICATE-----\\nMIICIjCCAcigAwIBAgIQcNHZPf7SM
   snpLbJvOgtUYjAKBggqhkjOPQQDAjBVMQsw\\nCQYDVQQGEwJERTEVMBMGA1UEChMMSHViamVjdCBHbWJIMRMwEQYKCZImiZPy
   LGQB\\nGRYDVjJHMRowGAYDVQQDExFWMkcgUm9vdCBDQSBRQSBHMTAeFw0yMjA0MDcxNDEx\\nMjBaFw0yNjA0MDcxNDExMjBa
   MEIxCzAJBgNVBAYTAkRFMRUwEwYDVQQKEwxIdWJq\\nZWN0IEdtYkgxHDAaBgNVBAMTE0NQTyBTdWIxIENBIFFBIEcxLjIwWTA
   TBgcqhkjO\\nPQIBBggqhkjOPQMBBwNCAAQu+9a26mDSIAgSACu3WCOth7bcQnJhqmMa+OYlCnc8\\n+QMhgl1wLS15agYgDpt
   dD5kJK+jt/CYRFZ4alwrXCf2po4GMMIGJMBIGA1UdEwEB\\n/wQIMAYBAf8CAQEwEQYDVR0OBAoECEAU+/DnqWOsMBMGA1UdIw
   QMMAqACEtF/4Il\\n/BCWMDsGCCsGAQUFBwEBBC8wLTArBggrBgEFBQcwAYYfaHR0cDovL29jc3AtcWEu\\naHViamVjdC5jb2
   06ODA4MDAOBgNVHQ8BAf8EBAMCAQYwCgYIKoZIzj0EAwIDSAAw\\nRQIhAL/4EvlWVR6+Z7+efMrttafXPoUfQWqqv1xIkGRo1
   wPQAiBbEmj7MeHZwV23\\nXPHkCjWCfzHwYlvQ4c8Cwo8ndW6law==\\n-----END CERTIFICATE-----\\n\"}"
  }
]
```

Example of a CertificateSignedRequest for OCPP 2.0.1:


```
[
 2,
 "123456789",
 "CertificateSigned",
 {
   "certificateType": "V2GCertificate",
   "certificateChain": "-----BEGIN CERTIFICATE-----\nMIICOjCCAeCgAwIBAgIQYVC3KfGq0abwLMaFjIDG+DAKBgg
   qhkjOPQQDAjBEMQsw\nCQYDVQQGEwJERTEVMBMGA1UEChMMSHViamVjdCBHbWJIMR4wHAYDVQQDExVDUE8g\nU3ViMiBDQSBR
   QSBHMS4yLjIwHhcNMjQwNzI0MTQwOTM1WhcNMjQxMDI0MTQwOTM1\nWjBxMQswCQYDVQQGEwJERTEVMBMGA1UEChMMSHViamV
   jdCBHbWJIMTYwNAYDVQQD\nEy1ERUlDRVNIVUJSRVFVSVJFTUVOVFNFVlNFQ0hFQ0tGT1JJU08xNTExODJQTkMx\nEzARBgoJ
   kiaJk/IsZAEZFgNDUE8wWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASM\nXvlrnbgJfTokmLl5EMGK7OG50SneeE94XUlZUTn
   1zG6X7ieXxzp9irz6DqjCpfNB\nv/uKSBWxA5FRFCSfhA1eo4GGMIGDMAwGA1UdEwEB/wQCMAAwEQYDVR0OBAoECE+u\nX7Ka
   VUZ3MBMGA1UdIwQMMAqACEeBskEROhG/MDsGCCsGAQUFBwEBBC8wLTArBggr\nBgEFBQcwAYYfaHR0cDovL29jc3AtcWEuaHV
   iamVjdC5jb206ODA4MDAOBgNVHQ8B\nAf8EBAMCA4gwCgYIKoZIzj0EAwIDSAAwRQIhAJzSjcMgpv8pKYk/oJB6g+5SLvv/\n
   fIajt/ybR6eOYg+xAiBuEoerEeQRFGsI0em02S9ylvsESrAvMVxIhfVwvQiPGA==\n-----END CERTIFICATE-----\n----
   -BEGIN CERTIFICATE-----\nMIICFTCCAbqgAwIBAgIQcowq33e0GXvgnfM3GEiJQjAKBggqhkjOPQQDAjBCMQsw\nCQYDVQ
   QGEwJERTEVMBMGA1UEChMMSHViamVjdCBHbWJIMRwwGgYDVQQDExNDUE8g\nU3ViMSBDQSBRQSBHMS4yMB4XDTI0MDIyODEzN
   Tg0NVoXDTI2MDQwNjEyNTg0NVow\nRDELMAkGA1UEBhMCREUxFTATBgNVBAoTDEh1YmplY3QgR21iSDEeMBwGA1UEAxMV\nQ1
   BPIFN1YjIgQ0EgUUEgRzEuMi4yMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE\nPHrw6dEPSV8YRpH2K3tkhS1Xn5AVRxZUl
   pPmuOFfPXkNciLe7O78Yasxd2Nmx02c\nXwa5UIg7HqWckwfHMLb0saOBjzCBjDASBgNVHRMBAf8ECDAGAQH/AgEAMBEGA1Ud
   \nDgQKBAhHgbJBETоRvzATBgNVHSMEDDAKgAhAFPvw56ljrDA+BggrBgEFBQcBAQQy\nMDAwLgYIKwYBBQUHMAGGImh0dHA6L
   y91cy5vY3NwLXFhLmh1YmplY3QuY29tOjgw\nODAwDgYDVR0PAQH/BAQDAgEGMAoGCCqGSM49BAMCA0kAMEYCIQDmnpai8pt6
   yGCr\nJzGdiybuSblVGbhBWmeyqP42h7C7YwIhAPnqxXMWbmnp1e81x0EK3JOLFbSNBL3a\nA8w9gmnaKX54\n-----END CE
   RTIFICATE-----\n-----BEGIN CERTIFICATE-----\nMIICIjCCAcigAwIBAgIQcNHZPf7SMsnpLbJvOgtUYjAKBggqhkjO
   PQQDAjBVMQsw\nCQYDVQQGEwJERTEVMBMGA1UEChMMSHViamVjdCBHbWJIMRMwEQYKCZImiZPyLGQB\nGRYDVjJHMRowGAYDV
   QQDExFWMkcgUm9vdCBDQSBRQSBHMTAeFw0yMjA0MDcxNDEx\nMjBaFw0yNjA0MDcxNDExMjBaMEIxCzAJBgNVBAYTAkRFMRUw
   EwYDVQQKEwxIdWJq\nZWN0IEdtYkgxHDAaBgNVBAMTE0NQTyBTdWIxIENBIFFBIEcxLjIwWTATBgcqhkjO\nPQIBBggqhkjOP
   QMBBwNCAAQu+9a26mDSIAgSACu3WCOth7bcQnJhqmMa+OYlCnc8\n+QMhgl1wLS15agYgDptdD5kJK+jt/CYRFZ4alwrXCf2p
   o4GMMIGJMBIGA1UdEwEB\n/wQIMAYBAf8CAQEwEQYDVR0OBAoECEAU+/DnqWOsMBMGA1UdIwQMMAqACEtF/4Il\n/BCWMDsGC
   CsGAQUFBwEBBC8wLTArBggrBgEFBQcwAYYfaHR0cDovL29jc3AtcWEu\naHViamVjdC5jb206ODA4MDAOBgNVHQ8BAf8EBAMC
   AQYwCgYIKoZIzj0EAwIDSAAw\nRQIhAL/4EvlWVR6+Z7+efMrttafXPoUfQWqqv1xIkGRo1wPQAiBbEmj7MeHZwV23\nXPHkC
   jWCfzHwYlvQ4c8Cwo8ndW6law==\n-----END CERTIFICATE-----\n"
 }
]
```

2.7 Securing the connection between EVSE and CPMS (processual)

ID	Requirement Definition
HUB-27-001	The connection between EVSE and CPMS in an untrusted network shall follow the security requirements regarding security profile 2 or higher as specified by section 1.3 “Security Profiles” of the OCPP 2.0.1 specification.
HUB-27-002	The EVSE shall have a corresponding CSMS Root Certificate installed to validate the CSMS leaf certificate.
OCPP 2.0.1: A00.FR.313	The Charging Station and CSMS shall only use TLS v1.2 or above.
OCPP 2.0.1: A00.FR.314	Both of these endpoints (Charging Station and CSMS) SHALL check the version of TLS used
OCPP 2.0.1: A00.FR.315	The CSMS detects that the Charging Station only allows connections using an older version of TLS, or only allows SSL. The CSMS SHALL terminate the connection
OCPP 2.0.1: A00.FR.319	The Charging Station SHALL support at least the cipher suites: (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 AND TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384) OR (TLS_RSA_WITH_AES_128_GCM_SHA256 AND TLS_RSA_WITH_AES_256_GCM_SHA384) Note 1: TLS_RSA does not support forward secrecy, therefore TLS_ECDHE is RECOMMENDED
HUB-27-003	Security Profile 1 as specified by section 1.3 “Security Profiles” of the OCPP 2.0.1 specification shall only be used in private networks using private APNs, VPNSs or similar.
HUB-27-004	The EVSE shall not use deprecated ciphers to connect to the CPMS.

2.8 Performing PnC related OCPP messages (processual)

2.8.1 Performing an OCPP Authorize Request with “iso15118CertificateHashData”

The EVSE provides the needed information for the OCSP request for the contract certificate chain to the CSMS in the OCPP Authorize Request message. With the provided information the CSMS is able to check the OCSP status for the contract certificate chain.

ID	Requirement Definition
HUB-281-001	The EVSE shall extract and respectively calculate the following attributes for each certificate of the Contract Certificate chain. • responderURL • hashAlgorithm • issuerNameHash • issuerKeyHash • serialNumber
HUB-281-002	The responderURL shall be extracted from the certificate’s “Authority Information Access” extension.
HUB-281-003	The EVSE shall provide in the “iso15118CertificateHashData” the “OCSPRequestDataType” for all certificates in the contract chain.
HUB-281-004	The EVSE shall include a maximum of four “iso15118CertificateHashData” elements in the OCPP Authorize Request.
HUB-281-005	The EVSE should provide the hash data for the whole contract certificate chain in the following order: Contract Leaf certificate MO Sub-CA 2 MO Sub-CA 1
HUB-281-006	It is recommended that the EVSE provides the contract certificate chain information to the CSMS as hash data instead of forwarding the certificate chain in .PEM format in the OCPP Authorize Request. Note: Sending the contract certificate chain as hash data will minimize the data traffic between EVSE and CPMS and speed up the validation process.

HUB-281-008	The EVSE shall be able to use the SHA-256 algorithm to calculate Issuer Name hash and Issuer Key hash for the contract certificate and MO chain.
HUB-281-009	It is recommended for better compatibility to use SHA-256 algorithm for calculating calculate Issuer Name hash and Issuer Key hash for the contract certificate and MO chain

Example of an Authorize.req message that only includes the certificate hash data for OCPP 1.6:


```
[
 2,
 "1234567890",
 "DataTransfer",
 {
  "vendorId":"org.openchargealliance.iso15118pnc",
  "messageId":"Authorize",
  "data":"{\"idToken\":{\"idToken\":\"DEICEREQUIRMNTS\"},
  \"iso15118CertificateHashData\":
  [{\"hashAlgorithm\":\"SHA256\",
  \"issuerNameHash\":\"5D9AA3B240912700F8621901B1FD95C73E2BDBAA00CCE071ADE233CD74A21DDC\",
  \"issuerKeyHash\":\"41D1DE817DDFA5EDD6D2AC64F98C70D25EC7B3842034D73F5E76A06839D0866A\",
  \"serialNumber\":\"5D05D7D15EB48A88D9E25CCC9D33E7E0\",
  \"responderURL\":\"http://ocsp-qa.hubject.com:8080\"},
  {\"hashAlgorithm\":\"SHA256\",
  \"issuerNameHash\":\"115C803CDCB2CBA1CC7D1EB3B20B069586FBC7F74EDA930347358E304C40355D\",
  \"issuerKeyHash\":\"7A9194FEF27EC5E8D95D3A668DE2E7686F3E92B1ADD28818CA02AF7408C57269\",
  \"serialNumber\":\"5DDF42CD0CBCF95C6942DF48C0DACE11\",
  \"responderURL\":\"http://ocsp-qa.hubject.com:8080\"},
  {\"hashAlgorithm\":\"SHA256\",
  \"issuerNameHash\":\"F53488037C9A84BBEBCE74C3BB5D175A36B6A41FF9F12E41A1C50A2FB7303159\",
  \"issuerKeyHash\":\"811B8014E48BA314127C5A54E79F841166C82ACD3CE2EB190EF7E25922F986DE\",
  \"serialNumber\":\"20EBA4FBC7C06F25D08B3055A52239E7\",
  \"responderURL\":\"http://ocsp-qa.hubject.com:8080\"}]}"
 }
]
```

Example of an AuthorizeRequest message that only includes the certificate hash data for OCPP 2.0.1:


```
[
 2,
 "1234567890",
 "Authorize"
 {
  "idToken":
   {
    "idToken": "DEICEREQUIRMNTS",
    "type":"eMAID"
   },
  "iso15118CertificateHashData": [
   {
    "hashAlgorithm": "SHA256",
    "issuerNameHash": "5D9AA3B240912700F8621901B1FD95C73E2BDBAA00CCE071ADE233CD74A21DDC",
    "issuerKeyHash": "41D1DE817DDFA5EDD6D2AC64F98C70D25EC7B3842034D73F5E76A06839D0866A",
    "serialNumber": "677410DD4902E668E205D14BF1FC06F2",
    "responderURL": "http://ocsp-qa.hubject.com:8080"
   },
   {
    "hashAlgorithm": "SHA256",
    "issuerNameHash": "115C803CDCB2CBA1CC7D1EB3B20B069586FBC7F74EDA930347358E304C40355D",
    "issuerKeyHash": "7A9194FEF27EC5E8D95D3A668DE2E7686F3E92B1ADD28818CA02AF7408C57269",
    "serialNumber": "5DDF42CD0CBCF95C6942DF48C0DACE11",
    "responderURL": "http://ocsp-qa.hubject.com:8080"
   },
   {
    "hashAlgorithm": "SHA256",
    "issuerNameHash": "F53488037C9A84BBEBCE74C3BB5D175A36B6A41FF9F12E41A1C50A2FB7303159",
    "issuerKeyHash": "811B8014E48BA314127C5A54E79F841166C82ACD3CE2EB190EF7E25922F986DE",
    "serialNumber": "20EBA4FBC7C06F25D08B3055A52239E7",
    "responderURL": "http://ocsp-qa.hubject.com:8080"
   }
  ]
 }
]
```


2.8.2. Performing an OCPP Authorize Request with the entire certificate chain in .PEM format

The EVSE could alternatively send an OCPP Authorize Request with the contract certificate chain in PEM format. The contract certificate chain includes the contract leaf certificate, MO Sub2-CA certificate, and MO Sub1-CA certificate. The difference between the OCPP Authorize Request including the entire certificate in PEM format and the OCPP Authorize Request only including the hash data as described in section **Error! Reference source not found.** is the information content that is transmitted to the CSMS.

Based on the certificates in the OCPP Authorize Request, the CSMS must calculate the necessary certificate hashes itself and perform the OCSP request. By sending the entire certificates to the CPMS, the CPMS is additionally able to validate the certificate chain itself.

Note: In the case that the OCPP Authorize Request only includes the hash data the validation of the certificate chain must be performed on EVSE side, since the CSMS does not have the necessary information to do so.

Note: Without the CentralContractValidationAllowed Configuration Variable/Key implemented the CSMS cannot determine how the OCPP Authorize Request will be formatted.

Note: Sending the contract certificate chain in .PEM format in the OCPP Authorize Request is not favorable since this increases the data traffic sent between EVSE and CPMS and increases the time for authorization.

ID	Requirement Definition
HUB-282-001	The EVSE shall implement the CentralContractValidationAllowed (ISO 15118 Related) Configuration Variable/Key in its device model if the contract certificate chain in .PEM format is included in the OCPP Authorize Request.
HUB-282-002	The EVSE may only use this mechanism when the corresponding MO Root certificate is not stored on the SECC and therefore the EVSE is not able to perform the validation of the certificate chain.
HUB-282-003	If the CentralContractValidationAllowed Configuration Variable/Key is not implemented, the EVSE shall send the OCPP Authorize Request including only the hash data.

Example of an Authorize.req message that only includes the certificate in PEM format for OCPP 1.6


```
[
 2,
 "1234567890",
 "DataTransfer",
 {
  "vendorId":"org.openchargealliance.iso15118pnc",
  "messageId":"Authorize",
  "data":"{\"idToken\":{\"idToken\":\"DEICEREQUIRMNTS\"},
  \"certificate\": \"-----BEGIN CERTIFICATE-----\\nMIIB+jCCAaCgAwIBAgIQZ3QQ3UkC5mjiBdFL8fwG8jAKBggqhkjOP
  QQDAjBDMQsw\\nCQYDVQQGEwJERTEVMBMGA1UEChMMSHViamVjdCBHbWJIMR0wGwYDVQQDExRNTyBT\\ndWIyIENBIFFBIEcxLjIuM
  TAeFw0yMzEyMjIxNTE5NDJaFw0yMzEyMzExMTAwMDBa\\nMC8xEzARBgNVBAoTCkVWU0UgQ0hFQ0sxGDAWBgNVBAMTD0RFSUNFUkVR
  VUlSTU5U\\nUzBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABM5dvcN7eKvaSmJjdRGCdgZcRYv1\\n5xDdgorM+SVF/w9jNw03Ayo/
  njhGDKlRv7//hDX5MMKSfYZMtc59aRYpka6jgYkw\\ngYYwDwYDVR0TAQH/BAUwAwEBADARBgNVHQ4ECgQITKOQ62d6+T4wEwYDVR0
  jBAww\\nCoAIRS5poTYibEgwOwYIKwYBBQUHAQEELzAtMCsGCCsGAQUFBzABhh9odHRwOi8v\\nb2NzcC1xYS5odWJqZWN0LmNvbTo
  4MDgwMA4GA1UdDwEB/wQEAwID6DAKBggqhkjO\\nPQQDAgNIADBFAiEA76u0wdefUateUX+p8NBbDY1bPomWzlieKXLo3HUh05gCIH
  6g\\nC0crZacGZCPuqBz/ymLKHm4Frf4Lp4+aHacz4hBp\\n-----END CERTIFICATE-----\\n-----BEGIN CERTIFICATE----
  -\\nMIICDzCCAbWgAwIBAgIQXd9CzQy8+VxpQt9IwNrOETAKBggqhkjOPQQDAjBBMQsw\\nCQYDVQQGEwJERTEVMBMGA1UEChMMSHV
  iamVjdCBHbWJIMRswGQYDVQQDExJNTyBT\\ndWIxIENBIFFBIEcxLjIwHhcNMjIwNDEwMjE1OTU5WhcNMzIwNDEwMjE1OTU5WjBD\\
  nMQswCQYDVQQGEwJERTEVMBMGA1UEChMMSHViamVjdCBHbWJIMR0wGwYDVQQDExRN\\nTyBTdWIyIENBIFFBIEcxLjIuMTBZMBMGBy
  qGSM49AgEGCCqGSM49AwEHA0IABGRs\\np5TTDIGpB+PEwmeG8D7Pgo/WN3U35Rxhe5ttLLlyF2jlmtOPHeHxWgGb0AO7H3L6\\nns
  o0A7Nn2KfDP8tG+OujgYwwgYkwEgYDVR0TAQH/BAgwBgEB/wIBADARBgNVHQ4E\\nCgQIRS5poTYibEgwEwYDVR0jBAwwCoAISw94E
  hgPO18wOwYIKwYBBQUHAQEELzAt\\nMCsGCCsGAQUFBzABhh9odHRwOi8vb2NzcC1xYS5odWJqZWN0LmNvbTo4MDgwMA4G\\nA1UdD
  wEB/wQEAwIBxjAKBggqhkjOPQQDAgNIADBFAiBqFxXTwnpm0eEgBPj/Px0k\\naEvZWdyZPm7BLJVJM6fT3QIhAKZPDhuau2DcN9xr
  rRPqqZLjfqPSMWw1D0VlCTqC\\nuv2k\\n-----END CERTIFICATE-----\\n-----BEGIN CERTIFICATE-----\\nMIICIjCCAc
  egAwIBAgIQIOuk+8fAbyXQizBVpSI55zAKBggqhkjOPQQDAjBVMQsw\\nCQYDVQQGEwJERTEVMBMGA1UEChMMSHViamVjdCBHbWJIM
  RMwEQYKCZImiZPyLGQB\\nGRYDVjJHMRowGAYDVQQDExFWMkcgUm9vdCBDQSBRQSBHMTAeFw0yMjA0MDcxNDEz\\nMDdaFw00MjA0M
  DcxNDEzMDdaMEExCzAJBgNVBAYTAkRFMRUwEwYDVQQKEwxIdWJq\\nZWN0IEdtYkgxGzAZBgNVBAMTEk1PIFN1YjEgQ0EgUUEgRzEu
  MjBZMBMGByqGSM49\\nAgEGCCqGSM49AwEHA0IABLWnWSw4NPNInduDQp6H0IFgeY0WtO0F3utqV191XLIe\\nspoAoSIz7s4Vhf+B
  hbbeX+UyftbGDp2m9EjGIBhog+mjgYwwgYkwEgYDVR0TAQH/\\nBAgwBgEB/wIBATARBgNVHQ4ECgQISw94EhgPO18wEwYDVR0jBAw
  wCoAIS0X/giX8\\nEJYwOwYIKwYBBQUHAQEELzAtMCsGCCsGAQUFBzABhh9odHRwOi8vb2NzcC1xYS5o\\ndWJqZWN0LmNvbTo4MDg
  wMA4GA1UdDwEB/wQEAwIBBjAKBggqhkjOPQQDAgNJADBG\\nAiEAsApDKLvPUVuDCtsIAnn/+prsGu5aekwd59tLiCHAFwACIQCFGJ
  HvTz7JUrq/\\nQJhQzehduW/+oaROsqOp8L3JdEO6XA==\\n-----END CERTIFICATE-----\\n\"}"
  }
]
```

Example of an AuthorizeRequest message that only includes the certificate in PEM format for OCPP 2.0.1:


```
[
 2,
 "1234567890",
 "Authorize"
 {
  "idToken":
   {
    "idToken": "DEICEREQUIRMNTS",
    "type":"eMAID"
   },
  "certificate": "-----BEGIN CERTIFICATE-----\nMIIB+jCCAaCgAwIBAgIQZ3QQ3UkC5mjiBdFL8fwG8jAKBggqhkjOPQQD
  AjBDMQsw\nCQYDVQQGEwJERTEVMBMGA1UEChMMSHViamVjdCBHbWJIMR0wGwYDVQQDExRNTyBT\ndWIyIENBIFFBIEcxLjIuMTAeF
  w0yMzEyMjIxNTE5NDJaFw0yMzEyMzExMTAwMDBa\nMC8xEzARBgNVBAoTCkVWU0UgQ0hFQ0sxGDAWBgNVBAMTD0RFSUNFUkVRVUlS
  TU5U\nUzBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABM5dvcN7eKvaSmJjdRGCdgZcRYv1\n5xDdgorM+SVF/w9jNw03AYo/njhGD
  KlRv7//hDX5MMKSfYZMtc59aRYpka6jgYkw\ngYYwDwYDVR0TAQH/BAUwAwEBADARBgNVHQ4ECgQITKOQ62d6+T4wEwYDVR0jBAww
  \nCoAIRS5poTYibEgwOwYIKwYBBQUHAQEELzAtMCsGCCsGAQUFBzABhh9odHRwOi8v\nb2NzcC1xYS5odWJqZWN0LmNvbTo4MDgwM
  A4GA1UdDwEB/wQEAwID6DAKBggqhkjO\nPQQDAgNIADBFAiEA76u0wdefUateUX+p8NBbDY1bPomWzlieKXLo3HUh05gCIH6g\nC0
  crZacGZCPuqBz/ymLKHm4Frf4Lp4+aHacz4hBp\n-----END CERTIFICATE-----\n-----BEGIN CERTIFICATE-----\nMIICD
  zCCAbWgAwIBAgIQXd9CzQy8+VxpQt9IwNrOETAKBggqhkjOPQQDAjBBMQsw\nCQYDVQQGEwJERTEVMBMGA1UEChMMSHViamVjdCBH
  bWJIMRswGQYDVQQDExJNTyBT\ndWIxIENBIFFBIEcxLjIwHhcNMjIwNDEwMjE1OTU5WhcNMzIwNDEwMjE1OTU5WjBD\nMQswCQYDV
  QQGEwJERTEVMBMGA1UEChMMSHViamVjdCBHbWJIMR0wGwYDVQQDExRN\nTyBTdWIyIENBIFFBIEcxLjIuMTBZMBMGByqGSM49AgEG
  CCqGSM49AwEHA0IABGRs\np5TTDIGpB+PEwmeG8D7Pgo/WN3U35Rxhe5ttLLlyF2jlmtOPHeHxWgGb0AO7H3L6\nnso0A7Nn2KfDP
  8tG+OujgYwwgYkwEgYDVR0TAQH/BAgwBgEB/wIBADARBgNVHQ4E\nCgQIRS5poTYibEgwEwYDVR0jBAwwCoAISw94EhgPO18wOwYI
  KwYBBQUHAQEELzAt\nMCsGCCsGAQUFBzABhh9odHRwOi8vb2NzcC1xYS5odWJqZWN0LmNvbTo4MDgwMA4G\nA1UdDwEB/wQEAwIBx
  jAKBggqhkjOPQQDAgNIADBFAiBqFxXTwnpm0eEgBPj/Px0k\naEvZWdyZPm7BLJVJM6fT3QIhAKZPDhuau2DcN9xrrRPqqZLjfqPS
  MWw1D0VlCTqC\nuv2k\n-----END CERTIFICATE-----\n-----BEGIN CERTIFICATE-----\nMIICIjCCAcegAwIBAgIQIOuk+
  8fAbyXQizBVpSI55zAKBggqhkjOPQQDAjBVMQsw\nCQYDVQQGEwJERTEVMBMGA1UEChMMSHViamVjdCBHbWJIMRMwEQYKCZImiZPy
  LGQB\nGRYDVjJHMRowGAYDVQQDExFWMkcgUm9vdCBDQSBRQSBHMTAeFw0yMjA0MDcxNDEz\nMDdaFw00MjA0MDcxNDEzMDdaMEExC
  zAJBgNVBAYTAkRFMRUwEwYDVQQKEwxIdWJq\nZWN0IEdtYkgxGzAZBgNVBAMTEk1PIFN1YjEgQ0EgUUEgRzEuMjBZMBMGByqGSM49
  \nAgEGCCqGSM49AwEHA0IABLWnWSw4NPNInduDQp6H0IFgeY0WtO0F3utqV191XLIe\nspoAoSIz7s4Vhf+BhbbeX+UyftbGDp2m9
  EjGIBhog+mjgYwwgYkwEgYDVR0TAQH/\nBAgwBgEB/wIBATARBgNVHQ4ECgQISw94EhgPO18wEwYDVR0jBAwwCoAIS0X/giX8\nEJ
  YwOwYIKwYBBQUHAQEELzAtMCsGCCsGAQUFBzABhh9odHRwOi8vb2NzcC1xYS5o\ndWJqZWN0LmNvbTo4MDgwMA4GA1UdDwEB/wQEA
  wIBBjAKBggqhkjOPQQDAgNJADBG\nAiEAsApDKLvPUVuDCtsIAnn/+prsGu5aekwd59tLiCHAFwACIQCFGJHvTz7JUrq/\nQJhQze
  hduW/+oaROsqOp8L3JdEO6XA==\n-----END CERTIFICATE-----\n"
 }
]
```

2.8.3. Certificate data handling

ID	Requirement Definition
HUB-283-001	The EVSE shall be able to use the SHA-256 algorithm to calculate the issuer name hash and the issuer key hash for the certificates that are provided in OCPP GetInstalledCertificateIds Response.
HUB-283-002	It is recommended for better compatibility to use the SHA-256 algorithm for calculating the issuer name hash and issuer key hash for the certificates that are provided in OCPP GetInstalledCertificateIds Response.
HUB-283-003	If the certificate type is “V2GCertificateChain” in the GetInstalledCertificateIds response, the EVSE shall provide the “childCertificateHashData” field with the data of the SECC Leaf Certificate chain in the following order: • CPO SUB-CA 2 • CPO SUB-CA 1.
HUB-283-004	It is recommended for better compatibility to be case insensitive when processing the data provided in the OCPP DeleteCertificate Request.

2.9 Coexistence of EIM Authentication and PnC Authentication (processual)

To respect and not overrule the explicit choice of authentication by the EV driver, the following requirement shall be fulfilled. This is being done to improve price transparency.

ID	Requirement Definition
HUB-29-001	If the EV driver uses External Payment (EIM) or other authentication methods at the EVSE for authorization purposes before plugging in the charge connector, the EVSE shall not offer "Contract" (PnC) as payment/authentication method in the ServiceDiscoveryRes message. [cf. ISO 15118 - 2] ExternalPayment refers to the following authentication methods: • RFID Card (UID) • "RemoteStart" (SMS, CallCenter, eMSP-App, EV-HMI, etc.) • Local authorization (debit/credit card)

Note: This requirement can only be fulfilled if the authorization is done before the cable is plugged in. As soon as the ServiceDiscoveryRes Message has been sent, the vehicle is free to decide.

Note: The authorization-idToken presented for the ExternalPayment method is only used for billing if the Vehicle is asking for EIM (ExternalPayment). If the vehicle chooses PnC (Contract), the Authorization and billing shall always be done with the EMAID of the contract certificate.

2.10 Contract Certificate Installation (processual)

The contract certificate is used to authenticate the user for an PnC charging session. The ISO15118 specifies the "Certificate Installation" and the "Certificate Update" process for installing new contract certificates to the EV respectively updating contract certificates in the EV.

Hubject's PnC Ecosystem only supports the certificate installation process as the adoption of the certificate update procedure in the field is very limited.

ID	Requirement Definition
HUB-210-001	The EVSE shall implement the certificate installation procedure as specified by ISO 15118-2.
HUB-210-002	The EVSE shall send the exi-payload of the CertificateInstallationReq, which it received from the EV, encoded in base64 to the CPMS. The V2GTP header shall be removed from the CertificateInstallationReq before.

Example of the field “exiRequest” in the OCPP Get15118EVCertificate Request. The field shall be base64 encoded EXI-Stream. The V2GTP Header is not included.


```
"exiRequest":"gJgCDR1/BvH7L0EKiVodHRwOi8vd3d3LnczLm9yZy9UUi9jYW5vbmljYWwtZXhpL0NWh0dHA6Ly93d3cudzMub3JnL
zIwMDEvMDQveG1sZHNpZy1tb3JlI2VjZHNhLXNoYTI1NkQQRsbSpMriBK0Ojo4HReXu7u7lzuZlze5M5eqKRexsLc3tzSxsLYWsrw0l6
QpaHR0cDovL3d3dy53My5vcmcvMjAwMS8wNC94bWxlbmMjc2hhMjU2QgfPWJPmrBCU4EWOVTn23fz6dc9GfyLw1s6JyH3Gt51cUSgHo8
MfNP7KUHPlG1GpCVCGjL3sfh6jbKoNlRGwtF47PRkN/yVWOO3S9byiaD+3qH/8j9pDhlUpSkFHoz1bSd1TqBQOxtKkyuJXAhhBARUYQQ
DoUAGBAIEBCCj894VUcXjnXJvPhKuR3y4YBQMEFUMkZx6CAYEYIhiFmASDAaqCAwmBIiKYipgJgwGqggUJhiQ6sTUysboQI7axJBiPGA
4DAaqCAYmKp6KmkCm6sRkQIaCQKKCQI5iXGRcYmA8LhpkZGJgYnJiZmZyZmi0LhpkbGJgYnJiZmZyZmi0YIZiIGAcDAaqCBQmDpDqxNT
KxuhiNGAwDAaqCAYmIpCqhKCknqyGiqSohJ6wooJiYiZgIgwUEyRNEyfkWMgCMiwGnoqaYLJgJgwOVQyRnHoEAgwQVQyRnHoGAg4GhAA
IvYR5EdeHqmHYMVa9w1NjuTqqEYdYwQ2gRe2ZuAVVCE7Z/+bwM/I36AaA2q2ihtOqH8tevI2lO+zdTMnyi11BB0cDSGEDQmAYDAaqOiY
CA/4IBGAAYCIMBqo6HAgUCBCctJjmuufBWGA4DAaqOiIIKmAnBCKQqoSgpJ6shoqkqISesKKCYmAmDAaqOkYIGGAVABCF0MjRdY2kQmB
2DBBWDAIKCg4CAgheYFpgVgwQVgwCCgoOYAMMPtDo6OB0Xl7exubgWuLCXNDqxNTKxuhcxt7adHBgcGBgHAwGqjoeAgP+CAgGBAcQYBQ
MEFUMkZx6CAYEBpAAYIoEQHQE4zeNElvqNELgUDsVE4dLgCHcwlH+9dzCTIhHn5ICBEIBV3g6n0IhWVAFK3WzaAVw6d5RiE6kG9oTcdV
WdUS2IUwCVDTj1WMkcgUm9vdCBDQSBRQSBHMSxPPUh1YmplY3QgR21iSA7cuzmK3TlMDOhf3em8u0gKvTARAA="
```


Example of the field “exiResponse” in the OCPP Get15118EVCertificate Response. The field shall be base64 encoded EXI-Stream.


```
"exiResponse":"gJgCDR1/BvH7L0EKiVodHRwOi8vd3d3LnczLm9yZy9UUi9jYW5vbmljYWwtZXhpL0NWh0dHA6Ly93d3cudzMub3Jn
LzIwMDEvMDQveG1sZHNpZy1tb3JlI2VjZHNhLXNoYTI1NkQMRpKIZASAtDo6OB0Xl7u7u5c7mZc3uTOXqikXsbC3N7c0sbC2FrK8NJekK
Wh0dHA6Ly93d3cudzMub3JnLzIwMDEvMDQveG1sZW5jI3NoYTI1NkIDsHg7CeXVxcS80YroqUfuJE+gDOcsjfrmh3dgjlk6TbBAxGkoh
iBK0Ojo4HReXu7u7lzuZlze5M5eqKRexsLc3tzSxsLYWsrw0l6QpaHR0cDovL3d3dy53My5vcmcvMjAwMS8wNC94bWxlbmMjc2hhMjU2
Qg3fg9LTZnit4xo2a3HtLAFCS+QNqtOZvYIpEIgu3tG+IEDEaSiGgErQ6OjgdF5e7u7uXO5mXN7kzl6opF7Gwtze3NLGwthayvDSXpCl
odHRwOi8vd3d3LnczLm9yZy8yMDAxLzA0L3htbGVuYyNzaGEyNTZCCYSvNSu3mLrxnra7bffP2lOUJGuv5nJYWaKQM9WtJOYwQMRpKIZ
gStDo6OB0Xl7u7u5c7mZc3uTOXqikXsbC3N7c0sbC2FrK8NJekKWh0dHA6Ly93d3cudzMub3JnLzIwMDEvMDQveG1sZW5jI3NoYTI1Nk
IPCrZnrWClHQh5Q1n3eL5rKUic2h5Mta45HXp0cKyQemEoDbcGQJW8jZW/RPggRM0QSnL0554twS0g1OqRCB038wiC4uefxbBZ3oUPt+
Zl+qp+WI02DZuk622P94cxCOPgEwgYAKiBDCCAh4wggHEoAMCAQICEGEUyC/vwkdLY1cRSZAWmVEwCgYIKoZIzj0EAwIwRTELMAkGA1U
EBhMCREUxFTATBgNVBAoTDEh1YmplY3QgR21iSDEfMB0GA1UEAxMWUHJvdiBTdWIyIENBIFFBIEcxLjIuMTAeFw0yMzA4MTcxNTU1NDV
aFw0yNzA4MTcxNTU1NDVaMFExCzAJBgNVBAYTAkVVMRUwEwYDVQQKEwxIdWJqZWN0IEdtYkgxFjAUBgNVBAMTDUNQUyAyMDIzLjggUUE
xEzARBgoJkiaJk/IsZAEZFgNDUFMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARnGUT0eeuxK7w3ticZsFKPz7aghbPvXZTSkQMecDZ
MatvDSmIog8Ew57eKApzm4ilpZQUt+zbCZODSTxecesOHo4GJMIGGMA8GA1UdEwEB/wQFMAMBAQAwEQYDVR0OBAoECE6fjsU31FFFMBM
GA1UdIwQMMAqACEb3artDbLe9MDsGCCsGAQUFBwEBBC8wLTArBggrBgEFBQcwAYYfaHR0cDovL29jc3AtcWEuaHViamVjdC5jb206ODA
4MDAOBgNVHQ8BAf8EBAMCB4AwCgYIKoZIzj0EAwIDSAAwRQIhAPLyE2YnLaDrDvjzfRH02UaH//G2Nw9kPBi67dRTuieCAiBeaRjUDPF
gdxtwhnfnI3RQPwtHAVWxrwf2mPgRCWD+wgTAIYQQEKGEEA3NABgQCBAQgu+vy/NQ130Jkph0XTzND8mAUDBBVDJGceggGBGCGYhZgEg
wGqggMJgSIimIqYCYMBqoIFCYYkOrE1MrG6ECO2sSQYjpgNgwGqggGJiig5N7sQKbqxGJAhoJAooJAjmJcZGA8LhpkZGBoYmBkYmpyan
K0LhpmYGBoYmBkYmpyanK0YIpiFmASDAaqCAwmBIiKYipgJgwGqggUJhiQ6sTUysboQI7axJBiPmA6DAaqCAYmLKDk3uxApurEZECGgk
CigkCOYlxkXGJgsmAmDA5VDJGcegQCDBBVDJGcegYCDgaEAAnqwstVYKr9RJSMrJARQoNW8px1umxEZRf4TsLwUnXrkr0f8keZMzVPv9
olHSygy2UJUpQA5UVaXC5sgT2ScEGnRwMYYQMSYCQMBqo6JgID/ggQYAwCA/4EAgBgIgwGqjocCBQIEI3u1XaG2W96YCYMBqo6RggYYB
UAEJrYNFk1CaGcYHYMEFYMAgoKDgICCF5gWmBWDBBWDAIKCg5gAww+0Ojo4HReXt7G5uBa4sJc0OrE1MrG6FzG3tp0cGBwYGAcDAaqOh
4CA/4ICAYEAgxgFAwQVQyRnHoIBgQGkgBgjARCAcjjKbGTQkgQuHG0sQg25P3U1YNWW19YzCDsfUh35HEuBEIBjZZzZ14/wtEgZc79Gw
zk+O1UGBWedUkxTU3olNTlwxAVAIYQQESGEEA5NABgQCBAQgHP5MRbWwOujjEEA1wt/hqmAUDBBVDJGceggGBGCqYhZgEgwGqggMJgSI
imIqYCYMBqoIFCYYkOrE1MrG6ECO2sSQYiZgIgwUEyRNEyfkWMgCMiwGrGSOYjRgMAwGqggGJiKsZI5ApN7e6ECGgkCigkCOYmA8Lhpk
ZGBoYG5iaGJoZGi0LhpmcGBoYG5iaGJoZGi0YIZiFmASDAaqCAwmBIiKYipgJgwGqggUJhiQ6sTUysboQI7axJBiOmA2DAaqCAYmKKDk
3uxApurEYkCGgkCigkCOYlxkYLJgJgwOVQyRnHoEAgwQVQyRnHoGAg4GhAAJncWh/a35fGyUeCu9NvTO5bKnhRCnUWTIWPY08qw4c73h
XGZkTa7yX4RC68CE+Pkf0nyXoJOhvaZJeCqRTu5FUUcDGGEDEmAkDAaqOiYCA/4IEGAMAgP+BAICYCIMBqo6HAgUCBCa2DRZNQmhnGAm
DAaqOkYIGGAVABCWi/8ES/ghLGB2DBBWDAIKCg4CAgheYFpgVgwQVgwCCgoOYAMMPtDo6OB0Xl7exubgWuLCXNDqxNTKxuhcxt7adHBg
cGBgHAwGqjoeAgP+CAgGBAIMYBQMEFUMkZx6CAYEBpIAYIwEQgGS4GkVpVXY50eFUjlKlt0SeFzU6V5oyYNdVZN3FQaisgRCAXyymSgG
24qcFhXRaOZslXv3rbCeq89fkf1VbHEBZP4eQBUlEMT+AzCCAfowggGgoAMCAQICEGd0EN1JAuZo4gXRS/H8BvIwCgYIKoZIzj0EAwIw
QzELMAkGA1UEBhMCREUxFTATBgNVBAoTDEh1YmplY3QgR21iSDEdMBsGA1UEAxMUTU8gU3ViMiBDQSBRQSBHMS4yLjEwHhcNMjMxMjIy
MTUxOTQyWhcNMjMxMjMxMTEwMDAwWjAvMRMwEQYDVQQKEwpFVlNFIENIRUNLMRgwFgYDVQQDEw9ERUlDRVJFUVVJUk1OVFMwWTATBgcq
hkjOPQIBBggqhkjOPQMBBwNCAATOXb3De3ir2kpiY3URgnYGXEWL9ecQ3YKKzPklRf8PYzcNNwGKP544RgypUb+//4Q1+TDCkn2GTLXO
fWkWKZGuo4GJMIGGMA8GA1UdEwEB/wQFMAMBAQAwEQYDVR0OBAoECEyjkOtnevk+MBMGA1UdIwQMMAqACEUuaaE2ImxIMDsGCCsGAQUF
BwEBBC8wLTArBggrBgEFBQcwAYYfaHR0cDovL29jc3AtcWEuaHViamVjdC5jb206ODA4MDAOBgNVHQ8BAf8EBAMCA+gwCgYIKoZIzj0E
AwIDSAAwRQIhAO+rtMHXn1GrXlF/qfDQWw2NWz6Jls5Ynily6Nx1IdOYAiB+oAtHK2WnBmQj7qgc/8piyh5uBa3+C6ePmh2nM+IQaQSY
IYQQEHmEEA2tABgQCBAQgu76Fmhl58rjShb6RgbWcImAUDBBVDJGceggGBGCCYhZgEgwGqggMJgSIimIqYCYMBqoIFCYYkOrE1MrG6EC
O2sSQYjZgMgwGqggGJiSankCm6sRiQIaCQKKCQI5iXGRgPC4aZGRgaGJgZGJqcmpytC4aZmRgaGJgZGJqcmpytGCGYhZgEgwGqggMJgS
IimIqYCYMBqoIFCYYkOrE1MrG6ECO2sSQYjpgNgwGqggGJiiankCm6sRkQIaCQKKCQI5iXGRcYmCyYCYMDlUMkZx6BAIMEFUMkZx6BgI
OBoQACMjZTymmGQNSD8eJhM8N4H2fBR+sbupvyjjC9zbaWXLkLtHLNaceO8PitAM3oAd2PuX1PZRoB2bPsU+Gf5aN8ddHAxhhAxJgJAw
GqjomAgP+CBBgDAID/gQCAGAiDAaqOhwIFAgQilzTQmxE2JBgJgwGqjpGCBhgFQAQlh7wJDAedr5gdgwQVgwCCgoOAgIIXmBaYFYMEFY
MAgoKDmADDD7Q6OjgdF5e3sbm4FriwlzQ6sTUysboXMbe2nRwYHBgYBwMBqo6HgID/ggIBgQDjGAUDBBVDJGceggGBAaQAGCKBEDULiu
nhPTNo8JACfH+fjpI0Jeys7kyfN2CWSqSZ0+nugRCAUyeHDc1dsG4b7jXWifVUyXG/UekYthqHorKEnUFdftIFMCGEEBERhBAOPQAYEA
gQEIEHXSfePgN5LoRZgq0pEc85gFAwQVQyRnHoIBgRgqmIWYBIMBqoIDCYEiIpiKmAmDAaqCBQmGJDqxNTKxuhAjtrEkGImYCIMFBMkT
RMn5FjIAjIsBqxkjmI0YDAMBqoIBiYirGSOQKTe3uhAhoJAooJAjmJgPC4aZGRgaGBuYmhiZmButC4aaGRgaGBuYmhiZmButGCCYhZgE
gwGqggMJgSIimIqYCYMBqoIFCYYkOrE1MrG6ECO2sSQYjZgMgwGqggGJiSankCm6sRiQIaCQKKCQI5iXGRgsmAmDA5VDJGcegQCDBBVD
JGcegYCDgaEAAlrTrJYcGnmkTu3BoU9D6ECwPMaLWnaC73W1K6+6rlkPWU0AUJEZ92cKwv/AwttvL/KZP2tjB07TeiRjEAw0QfTRwMYY
QMSYCQMBqo6JgID/ggQYAwCA/4EAgJgIgwGqjocCBQIEJYe8CQwHna+YCYMBqo6RggYYBUAEJaL/wRL+CEsYHYMEFYMAgoKDgICCF5gW
mBWDBBWDAIKCg5gAww+0Ojo4HReXt7G5uBa4sJc0OrE1MrG6FzG3tp0cGBwYGAcDAaqOh4CA/4ICAYEAgxgFAwQVQyRnHoIBgQGkgBgj
ARCAWAUhlF3nqK3BhW2EATz//U12DXctPSYO8+2lxBDgC4ABEIBCjEj3p59kqV1foEwoZvQu3Lf/UNInWVHU+F7kuiHdLhAKkohkMHzC
bBfho8UitwF6On7+AKONseH8wCI8cXLntIFYxD+3znd96FPorYvAn97+XIFZCwCpKIZkEEg75AVwmGbF9MJNZUR2/6Yln1gQ/IkeIPm8
XChoxfAhswliLjGmtWX6ogzuW2d//VXw3FX7F6MfU6PzZ3xoX/7QCpKIaBFERUlDRVJFUVVJUk1OVFMAA=="
```

2.11 OCPP compliance (processual)

ID	Requirement Definition
HUB-211-001	The EVSE shall be compliant to at least one of the following protocols: • OCPP 1.6 • OCPP 2.0.1
HUB-211-002	For the OCPP 1.6 the EVSE shall be compliant to OCPP 1.6 extension for Plug&Charge called “Using ISO 15118 Plug & Charge with OCPP 1.6” published by the OCA.

2.12 Deviation from OCPP Message Get15118EVCertificate (processual)

The value of the FIELD NAME *exiRequest/Response* in the OCPP Message Get15118EVCertificate is limited to 5600 characters. This limit is too low.

ID	Requirement Definition
HUB-212-001	The EVSE shall accept strings for *exiRequest/Response* being up to 7500 characters.

2.13 Securing local maintenance interface (processual)

Most chargers have a local interface for technicians and engineers to maintain the chargers or for local troubleshooting in the event of problems in the field (e.g local web server running on the charging station that can be accessed via ethernet)

ID	Requirement Definition
HUB-213-001	It is recommended that the local interface for debugging and maintaining the EVSE is secured via password and username.
HUB-213-002	It is recommended, that the password and username of the local interface are unique for each charger.
HUB-213-003	It is recommended, that the user is prompted to change the password and username of the local interface after initial log in.
HUB-213-004	It is recommended, that the application shall automatically log out users after 30 minutes of inactivity.

Note: The use of default username and password credentials to access the local interface of the charger presents security risks, as it may facilitate unauthorized access by malicious third parties. Without ensuring that the CPO (Charge Point Operator) changes the default credentials before deploying the chargers, sensitive information may be exposed, or malicious configurations could compromise the safety of charging operations. It is imperative to prioritize the implementation of unique and secure credentials for each charger's local interface to mitigate these risks effectively.

3 Technical Security Controls from the Hubject Certificate Policy (security)

3.1 Key Pair Generation, Installation and Usage

ID	Requirement Definition
HUB-31-001	End-entity keys for the SECC-Leaf-Certificate shall be generated on the subject (EVSE) device.
HUB-31-002	SECC-Leaf private keys shall not be removed from the device on which they were generated.
HUB-31-003	If SECC-Leaf private keys are removed from the device they are generated on, they shall be transferred in a secure way using a non-deprecated cipher.
HUB-31-004	If multiple SECC-Leaf-Certificates are needed (e.g for charger with multiple connectors) multiple CSRs with the same Common Name but with unique serial numbers and public keys shall be generated.
HUB-31-005	The EVSE/SECC-Leaf-Certificates keys and attributes shall be used according to the appropriate certificate usage specified in the certificate profiles in the ISO 15118 -2 Annex F.
HUB-31-006	The Common Name (CN) of the Subject shall be the SECCID of the charge point. The SECCID needs to follow the syntax of ISO 15118-20. Note: The Common Name shall be set to the SECCID as defined in ISO 15118-20 since in ISO 15118-2 the content of the Common Name was not formally defined.

HUB-31-007	SECCID shall be an alphanumeric string with a length of maximum 64 characters (i.e. A..Z, a..z, 0..9),
	
	• <SECCID> =
	<Country Code> <S> <EVSE Operator ID> <S> <ID Type> <S> <ControllerID> <S> <Check Digit>
	  ○ <Country Code> = 2 ALPHA; two-character country code according to ISO 3166-1 (Alpha-2-Code)
	  ○ <EVSE Operator ID> = 3 (ALPHA / DIGIT); three alphanumeric characters, referring to the EVSE Operator
	  ○ <ID Type> = “S”; one character “S” indicating that this ID represents a reference to a “Supply Equipment”
	  ○ <ControllerID> = Minimum 32 (ALPHA / DIGIT) Alphanumeric characters referring to the specific communication controller
	  ○ <Check Digit> = *1 (ALPHA / DIGIT); (optional) Used to verify valid SECCID
	
	Formatting
	• ALPHA = %x41-5A / %x61-7A; according to IETF RFC 5234 (7-Bit ASCII), case-insensitive (IETF RFC 7405)
	• DIGIT = %x30-39; according to IETF RFC 5234 (7-Bit ASCII)
	• <S> = *1 (“-”); optional separator, but advised not to use it between IT systems and only for visibility purposes
	Example
	• DEICES00003C4NABBB55787867564533096754347 6
	
	Note: The ISO15118-20 incorrectly specifies that the SECCID may be a maximum of 255 characters long. This is not possible since the Common Name of a Certificate Signing Request (CSR) is specified to be maximum 64 characters in RFC 5280. Most Crypto Libraries such as OpenSSL which are commonly used to create CSR on embedded systems will reject creating CSRs with a CN longer than 64 characters.
	
	Note: The hyphen character “-“, even though only used to increase the readability of the SECCID, is counted as one character. The hyphen must therefore be taken into account when creating the CSR. It is recommended not to use the hyphen to increase interoperability.

3.3 Transmission of Root CA certificates to trusting parties

ID	Requirement Definition
HUB-33-001	The public key and the certificate of the V2G Root CA(s) shall be stored by each SECC. The CPMS shall use a second communication channel for validating the V2G Root CA Certificate fingerprint, before installing it at the end-entities.
HUB-33-003	The SECC shall implement a way for the CPMS to securely install new root certificates without the danger of manipulation by adversaries. Note, the SECC cannot ensure the integrity and authenticity of the certificate on the way from the Root Certificate Pool to the CPMS but shall offer the functionality to the CPMS to ensure the integrity and authenticity of the certificate on the way from CPMS to the SECC.

3.5 OCSP requests of CPO Sub2-/ and Sub1-CA and OCSP Multi-Stapling

According to requirement [V2G2-070] and [V2G2-875] in ISO 15118-2, the EVCC must verify the certificate chain of the SECC certificate and the OCSP responses (including OCSP Signer certificates) of the SECC certificate chain. The SECC must provide all necessary OCSP responses in the TLS initialization response by means of OCSP stapling according to [RFC6961].

However, according to ietf.org the status_request_v2 extension [RFC6961] is deprecated. This extension was intended to be used for the EVCC checking the OCSP response for the CPO Sub2-/ and Sub1-CA.

Feedback from the market is such that currently no EV has implemented this check due to the missing mechanisms in TLS 1.2.

ID	Requirement Definition
HUB-35-001	The EVSE may request the Certificate status of the CPO chain via OCSP with the OCPP GetCertificateStatus Request message.
HUB-35-003	The EVSE shall cache the OCSP response as described in the “Next Update” Field of the OCSP Response or at least once a week (7 days) as required in ISO15118-2 (V2G2-649) before requesting a new certificate status. MIN(OCSP-Cache Requirement;7 days)
HUB-35-004	If the EV requests the certificate status for the CPO chain during the TLS handshake the EVSE shall request the certificate status via OCSP to ensure interoperability.

References

- S. Chokani et. al.: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, RFC 3647, November 2003
- IETF: Network Working Group, RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, 1997
- FIPS PUB 140-2, "Security Requirements for Cryptographic Modules", May 2001
- RFC 2560, X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP. M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, 1999.
- RFC 2986, PKCS #10: Certification Request Syntax Specification Version 1.7. M. Nystrom, B. Kaliski, D. Solo, 2000.
- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.
- ITU-T Recommendation X.501 (2005), Information technology - Open Systems Interconnection - The Directory: Models, 2008.
- ISO 15118-2:2014 Road vehicles — Vehicle-to-Grid Communication Interface — Part 2: Network and application protocol requirements.
- OCPP 2.0.1 Edition 3, Open Charge Alliance, 2024
- “Using ISO 15118 Plug & Charge with OCPP 1.6”, Open Charge Alliance, 2020
- OCPP 1.6 Edition 2 FINAL, Open Charge Alliance, 2017
- VDE Anwendungsregel: VDE-AR-E 2802-100-1 Anwendungsregel: 2019-12 Zertifikats-Handhabung für Elektrofahrzeuge, Ladeinfrastruktur und Backend-Systeme im Rahmen der Nutzung von ISO 15118