OCPP 1.6

ISO 15118 Extension

Version 1.3

2019-10-29

Roland Angerer, Christian Zellot, Mario Madej, Lisa Steiner

Table of Contents

Scope

This document describes an extension to the OCPP 1.6J protocoll to enable the necessary communication between EV and CSMS to support the ISO 15118 norm.

The general intention is to back-port the ISO 15118-specific messages from the OCPP 2.0 protocol into the OCPP 1.6J protocol using DataTransfer messages.

To simplify the initial implementation and speed up the adaption of ISO 15118 we will leave out the smart charging capabilities for now.

Abbreviations

Abbreviation	Description
CA	Certificate Authority
CSMS	Charging station management system
CSR	Certificate Signing Request
EV	Electrical vehicle
EVCC	EV Communication Controller
OCSP	Online Certificate Status Protocol
V2G	Vehicle to Grid

Scenarios

As this extension aims to back-port the ISO15118-specific messages from OCPP 2.0 to OCPP 1.6J the corresponding ISO15118 use cases are described in detail in the OCPP 2.0 Specification.

Please resort to the following OCPP 2.0 Specification sections for further details

- A. Security
- M. ISO 15118 CertificateManagement

Update Charging Station Certificate

An update of the charging station certificate (used for TLS communication between the EV and the charging station) can either be requested by the charging station via a SignCertificate DataTransfer message or triggered by the CSMS via a TriggerMessage call.

Initiated by the charging station

1. Charging station sends SignCertificate message to CSMS
2. CSMS asks CA to sign the corresponding CSR
3. CSMS sends the resulting certificate via CertificateSigned message to the charging station

See OCPP 2.0 Specification – A. Security Use case A03 for further details.

Initiated by the CSMS

1. CSMS sends ExtendedTriggerMessage call to charging station
2. Charging station sends SignCertificate message to CSMS
3. CSMS asks CA to sign the corresponding CSR
4. CSMS sends the resulting certificate via CertificateSigned message to the charging station

See OCPP 2.0 Specification – A. Security Use case A02 for further details.

EV Certificate Installation

When an EV wants to install a new certificate it will ask the charging station to retrieve a ISO 15118 compliant certificate. The charging station can use a Get15118EVCertificate DataTransfer message to retrieve such a certificate.

1. Charging station sends Get15118EVCertificate message to CSMS
2. CSMS retrieves corresponding certificate
3. CSMS responds with corresponding certificate

See OCPP 2.0 Specification – M. ISO 15118 CertificateManagement Use case M01 for further details.

Note: OCPP 2.0 also allows for a certificate update via Update15118EVCertificate, but we will simply always use Get15118EVCertificate for this extension.

Manage Charging Station Certificates

OCPP 2.0 allows the CSMS to manage the installed certificates of a charging station via the following calls:

- GetInstalledCertificateIds – retrieve list of currently installed certificates
- DeleteCertificate – delete a specific certificate
- InstallCertificate – install a specific certificate
- GetCertificateStatus – retrieve OCSP certificate status for charging station certificate

See OCPP 2.0 Specification – M. ISO 15118 CertificateManagement Use cases M02 to M06.

Messages

All messages will be implemented using OCPP 1.6J DataTransfer messages.

The following blueprint will be used for requests:

```
[
	2,
	"<UniqueId>",
	"DataTransfer",
	{
		"vendorId": "iso15118",
		"messageId": "<Action>",
		"data": "<Payload>"
	}
]
```

As we are using DataTransfer messages to encapsulate the corresponding messages, responses should always return status „Accepted“ unless the message could not be parsed:

```
[
	3,
	"<UniqueId>",
	{
		"status": "Accepted",
		"data": "<Payload>"
	}
]
```

Further details on the actual message can be given in the payload.

Authorize

In order to support the needed certificate details to properly authorize a charging process the charging station will need to use an Authorize DataTransfer message:

```
{
	"idToken": {
		"idToken": "<EVs eMAID>",
		"type": "eMAID"
	},
	"15118CertificateHashData": [{
		"hashAlgorithm": "SHA256|SHA384|SHA512",
		"issuerNameHash": "<issuer name>",
		"issuerKeyHash": "<issuer key>",
		"serialNumber": "<serial number>",
		"responderURL": "<responder URL>" // optional
	}, … ]
}
```

Field	Type	Description
15118CertificateHashData	OCSPRequestDataType[1..4]	See OCPP 2.0 Data Types

The CSMS will respond with the following message:

```
{
      "certificateStatus": "Accepted|CertificateRevoked",
      "idTokenInfo": {
            "status": "<status>",
            "cacheExpiryDateTime": "<expiry date and time>" // optional
      }
}
```

Field	Type	Description
certificateStatus	CertificateStatusEnumType	see OCPP 2.0 Enumerations
status	AuthorizationStatusEnumType	see OCPP 2.0 Enumerations
cacheExpiryDateTime	dateTime	Date and Time after which the token must be considered invalid.

CertificateSigned

The CertificateSigned DataTransfer message is used by the CSMS to inform the charging station of a successful certificate signing request (usually transmitted via SignCertificate):

```
{
      "cert": "<certificate>",
      "typeOfCertificate": <type> // optional
}
```

Field	Type	Description
cert	string[0..800]	The signed X.509 certificate, first DER encoded into binary, and then hex encoded into a case insensitive string. This can also contain the necessary sub CA certificates. In that case, the order should follow the certificate chain, starting from the leaf certificate.
typeOfCertificate	CertificateSigningUseEnumType	See OCPP 2.0 CertificateSigningUseEnumType

The charging station will respond with the following message:

```
{
      "status": "Accepted|Rejected"
}
```

DeleteCertificate

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 using a DeleteCertificate DataTransfer message:

```
{
      "certificateHashData": {
            "hashAlgorithm": "SHA256|SHA384|SHA512",
            "issuerNameHash": "<issuer name>",
            "issuerKeyHash": "<issuer key>",
            "serialNumber": "<serial number>"
      }
}
```

Field	Type	Description
certificateHashData	CertificateHashDataType	see OCPP 2.0 Data Types

The charging station will respond with the following message:

```
{
      "status": "Accepted|Failed|NotFound"
}
```

Get15118EVCertificate

If an ISO 15118 vehicle selects the service Certificate installation the charging station can use the Get15118EVCertificate DataTransfer message:

```
{
      "15118SchemaVersion": "<schema version>",
      "exiRequest": "<certificate installation request>"
}
```

Field	Type	Description
15118SchemaVersion	string[0..50]	Schema version currently used for the 15118 session between EV and Charging Station. Needed for of the EXI stream by the CSMS.
exiRequest	string[0..5500]	Raw CertificateInstallationReq request from EV, Base64 encoded.

The CSMS will respond with the following message:

```
{
```

```
      "status": "Accepted|Failed",
      "exiResponse": "<certificate installation response>",
      "contractSignatureCertificateChain": {
            "certificate": "…",
            "childCertificate": "…"
      },
      "saProvisioningCertificateChain": {
            "certificate": "…",
            "childCertificate": "…"
      }
}
```

Field	Type	Description
status	Accepted|Failed	Indicates whether the message was processed properly.
exiResponse	string[0..5500]	Raw CertificateInstallationRes response for the EV, Base64 encoded.
contractSignatureCertificateChain	CertificateChainType	See OCPP 2.0 Data Types
saProvisioningCertificateChain	CertificateChainType	See OCPP 2.0 Data Types

GetCertificateStatus

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 GetCertificateStatus DataTransfer message:

```
{
      "ocspRequestData": {
            "hashAlgorithm": "SHA256|SHA384|SHA512",
            "issuerNameHash": "<issuer name>",
            "issuerKeyHash": "<issuer key>",
            "serialNumber": "<serial number>",
            "responderURL": "<responder URL>" // optional
      }
}
```

Field	Type	Description
ocspRequestData	OCSPRequestDataType[1..4]	See OCPP 2.0 Data Types

The CSMS will respond with the following message:

```
{
      "status": "Accepted|Rejected",
      "ocspResult": "<OCSP response>" // optional
}
```

Field	Type	Description
ocspResult	string[0..5500]	OCSPResponse class as defined in IETF RFC 6960. DER encoded (as defined in IETF RFC 6960), and then base64 encoded.

GetInstalledCertificateIds

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 via a GetInstalledCertificateIds DataTransfer message:

```
{
      "typeOfCertificate": "CSMSRootCertificate"
}
```

Field	Type	Description
typeOfCertificate	CertificateUseEnumType	see OCPP 2.0 Enumerations

The charging station will respond with the following message:

```
{
      "status": "Accepted|NotFound",
      "certificateHashData": [{
            "hashAlgorithm": "SHA256|SHA384|SHA512",
            "issuerNameHash": "<issuer name>",
            "issuerKeyHash": "<issuer key>",
            "serialNumber": "<serial number>"
      }, … ]
}
```

Field	Type	Description
certificateHashData	CertificateHashDataType[0..*]	see OCPP 2.0 Data Types

InstallCertificate

In order to install a new root CA certificate, Sub-CA certificate for an eMobility Operator, Charging Station operator, or a V2G root certificate into the charging station the CSMS can use an InstallCertificate DataTransfer request:

```
{
      "certificateType": "CSMSRootCertificate",
      "certificate": "<certificate>"
}
```

Field	Type	Description
certificateType	CertificateUseEnumType	see OCPP 2.0 Enumerations
certificate	string[0..800]	An X.509 certificate, first DER encoded into binary, and then hex encoded into a case insensitive string.

The charging station will respond with the following message:

```
{
      "status": "Accepted"
}
```

Field	Type	Description
status	CertificateStatusEnumType	see OCPP 2.0 Enumerations

SignCertificate

Sent by the Charging Station to the CSMS to request that the Certificate Authority signs the public key into a certificate.

The charging station can use the SignCertificate DataTransfer message to receive a signed certificate:

```
{
      "csr": "<certificate signing request>",
      "typeOfCertificate": <type> // optional
}
```

Field	Type	Description
csr	string[0..800]	The Charging Station SHALL send the public key in form of a Certificate Signing Request (CSR) as described in the X.509 standard.
typeOfCertificate	CertificateSigningUseEnumType	See OCPP 2.0 CertificateSigningUseEnumType

The CSMS will respond with the following message:

```
{
      "status": "Accepted|Rejected"
}
```

The CSMS will forward the CSR to the corresponding CA and after being signed a CertificateSigned DataTransfer message will be sent to the charging station.

Update15118EVCertificate

Not implemented – simply use Get15118EVCertificate instead.

ExtendedTriggerMessage

This message is both based on the OCPP 2.0 TriggerMessageRequest (for SignChargingStationCertificate) and the OCPP 1.6J – improved security extension (for SignV2GCertificate).

In order to allow the CSMS to initiate a certificate update of the charging station, the CSMS will need to use a ExtendedTriggerMessage DataTransfer message:

```
{
      "requestedMessage": "SignChargingStationCertificate|SignV2GCertifcate"
}
```

The charging station will respond with the following message:

```
{
      "status": "Accepted|Rejected|NotImplemented"
}
```

In case of accepting the ExtendedTriggerMessage the charging station is going to send a SignCertificate request to update its certificate afterwards and will continue with the Update Charging Station Certificate „Initiated by the charging station“.