P3
PLUG & CHARGE TRAINING

Agenda

1 **Some Basics regarding ISO 15118**

2 **ISO 15118 Structure**

3 **Not described within ISO 15118 but required**

Agenda

1 **Some Basics regarding ISO 15118**

2 **ISO 15118 Structure**

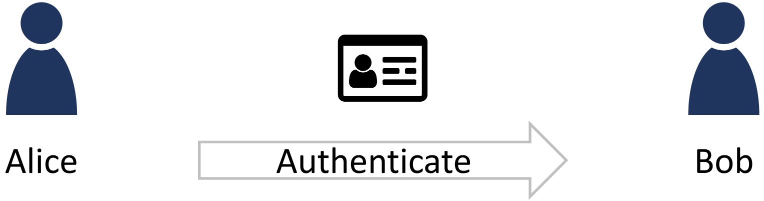
3 **Not described within ISO 15118 but required**

KEY SECURITY ASPECTS

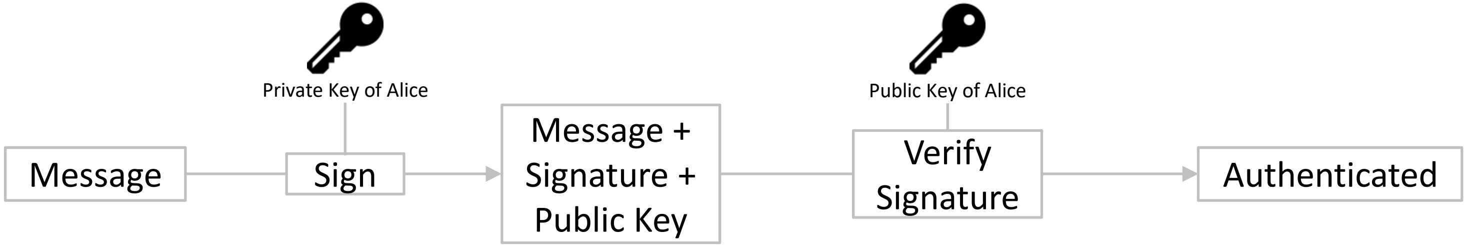
Cryptography bases on 3 principles to ensure a safe and secure communication between allowed participants

Confidentiality	Ensuring only allowed recipents read the message	**Asymmetric Cryptography** (different key pairs)
Integrity	Ensuring sent messages are not manipulated	**XML Signatures** (hash values)
Authenticity	Validation of recipents	**XML Signatures** (hash values)

The „Alice“ and „Bob“ scenario is a generic way to explain used cryptographical methods which are also relevant for ISO 15118

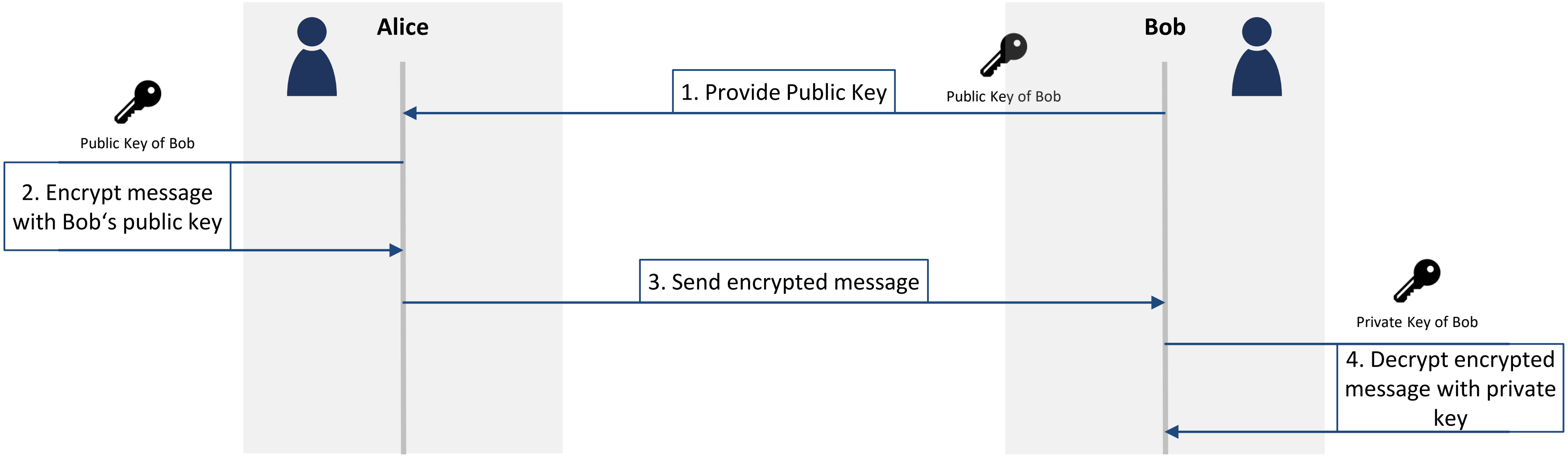


Analog:
To say who you are, you leave a signature at the bottom of a message. Alice authenticates herself in front of Bob, leaving her signature in the message.



Digital:
Within asymetric encryption there are key pairs, the public and the private key. A digital signature can only be created with the private key, which is used for authenticity and integrity as seen in the example where Alice idenfities her in front of Bob. Thats why the private key needs to be kept highly secure.

Encryption 1o1 – How to use public and private keys for confidentiality


Alice
Bob
1. Provide Public Key
Public Key of Bob
Public Key of Bob
2. Encrypt message with Bob‘s public key
3. Send encrypted message
Private Key of Bob
4. Decrypt encrypted message with private key

Alice wants to send Bob a secret message.

1. Bob provides Alice his public key.
2. Alice encrypts the message with Bobs public key.
3. Alice sends the encrypted message to Bob.
4. Bob decrypts the encrypted message from Alice.

ISO 15118 USE CASES

Next to precise charging scheduling, ISO 15118 includes a variety of new charging relevant use cases.

Potential additional use cases

Energie-Rückspeisung

- HEMS Anwendung
- Netzoptimierung
- Flotten Laden

DC Ladekontrolle

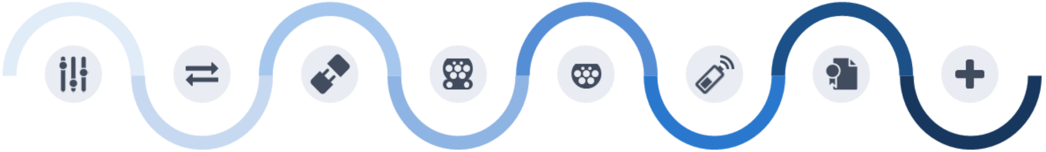
- Lade-Transparenz
- Planung von Ladezeiten

Induktive Ladekontrolle

- Kundenfreundlich
- Fine positioning
- Sicherer Datenaustausch

Value Added Services

- Zusätzliche Lade-Details
- Fahrzeug Services
- Location Based Services



Optimiertes Lastmanagement (Hauptanwendung)

- Überlast Schutz
- Optimiertes Laden
- Flotten Laden

Automatisierter Verbindungsaufbau

- Plug&Charge
- Fein-Positionierung
- Sicherer Aufbau der Kommunikation (TLS)

AC Ladekontrolle

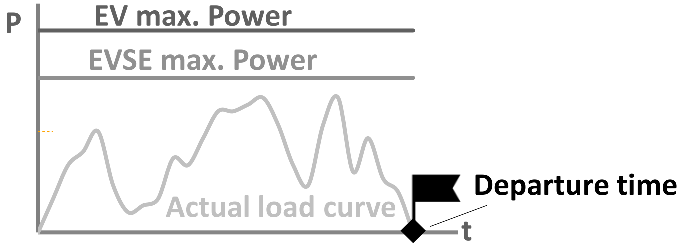
- Lade-Transparenz
- Planung von Ladezeiten

Einfache Bezahlung und Abrechnung

- Kundenfreundliche, einfache Abrechnung

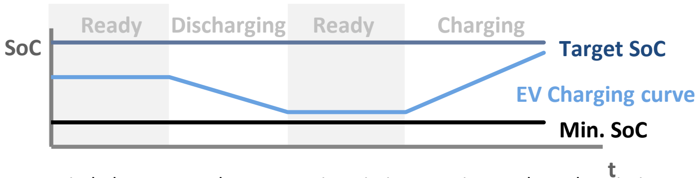
Charging use cases

Steuerung AC/DC Laden



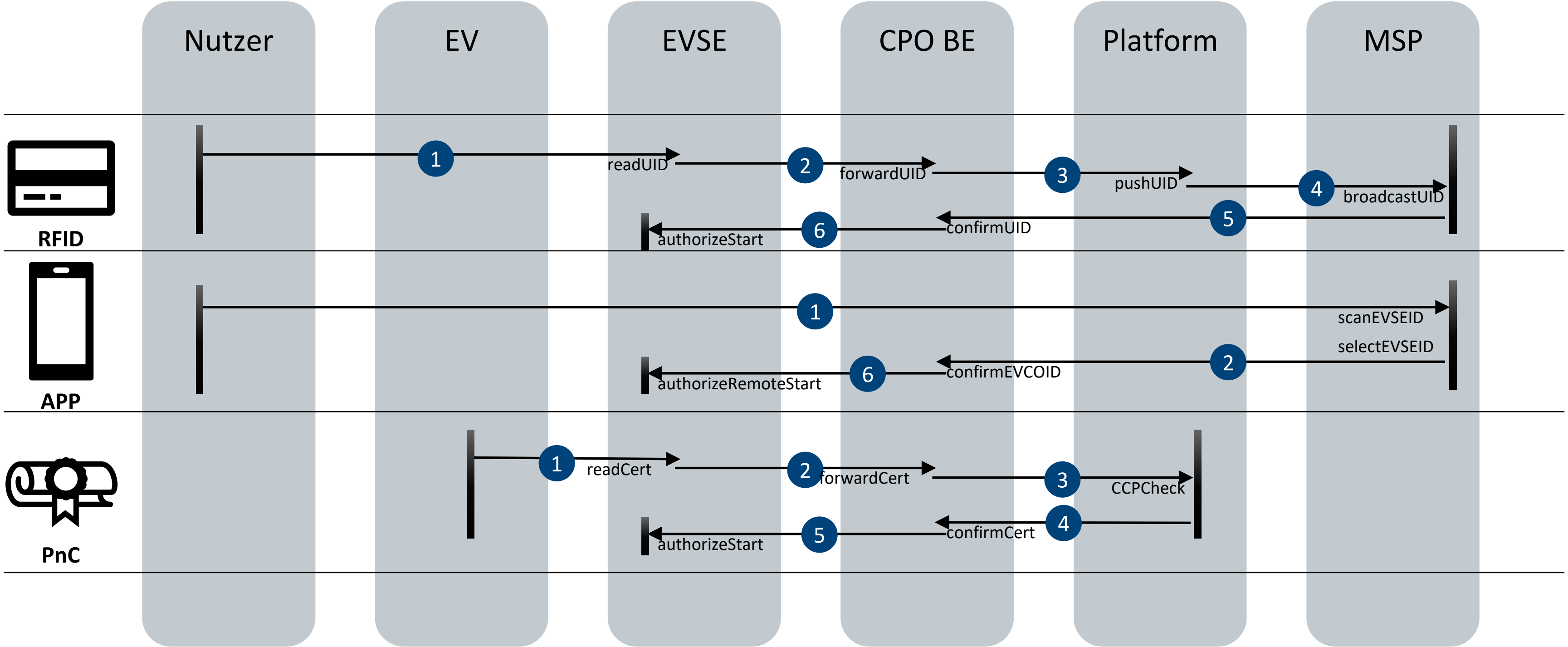
- Definition Abfahrtszeitpunkt und notwendiger SOC
- Reaktionsmöglichkeit auf variierende Tag-/Nachttaríe
- Abstimmung mit weiteren Verbrauchern im Haushalt und Netzentlastung

Bi-direktionales Laden (ab Edition 2.0)



- Heimladen: Netzentlastung, Preisoptimierung, Eigenverbrauchoptimierung
- Flottenladen: V2V Steuerung und Priorisierung der Ladevorgänge

Authentication methods differ only slightly from a technical flow perspective. Enabler technology however is a completely different story.

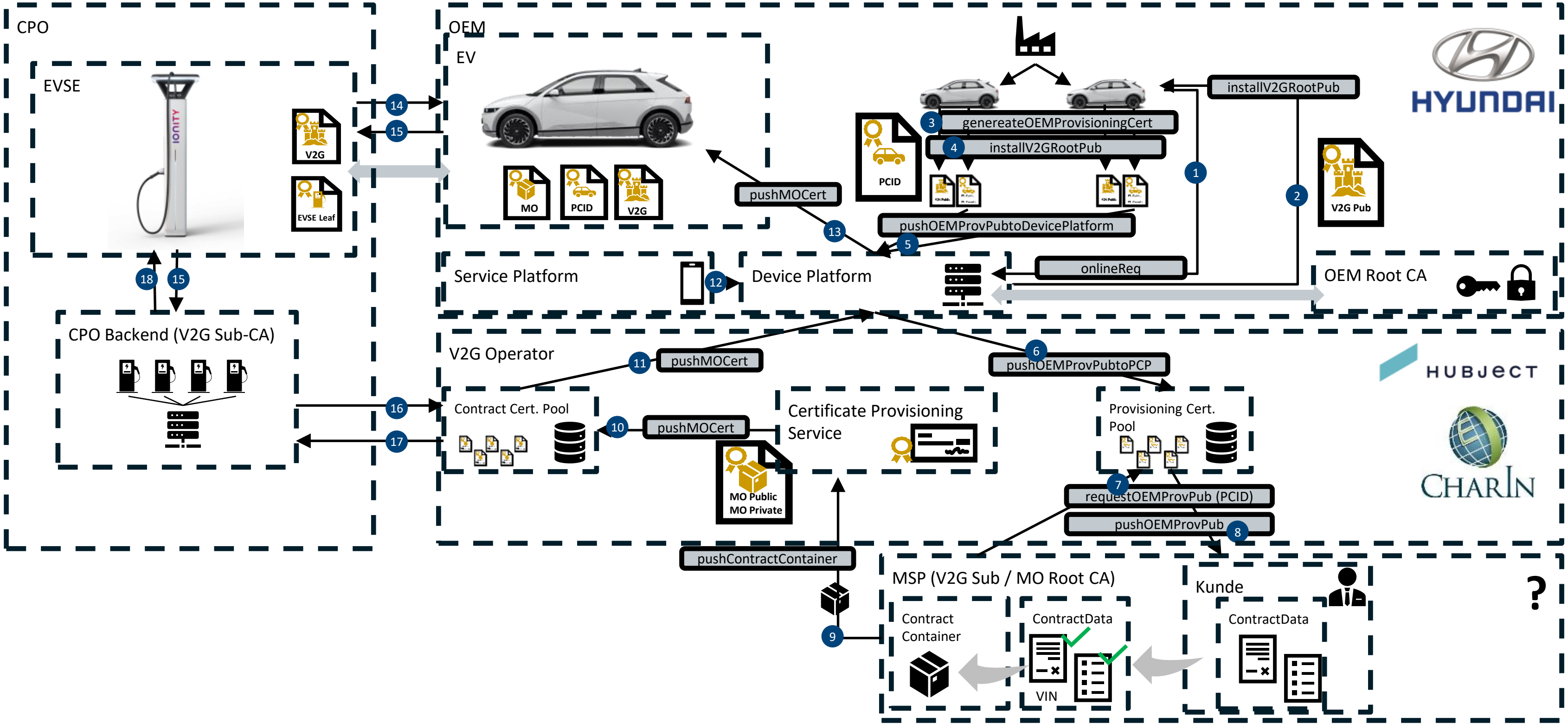


AUTHENTICATION COMPARISON

Authentication methods differ only slightly from a technical flow perspective. Enabler technology however is a completely different story.

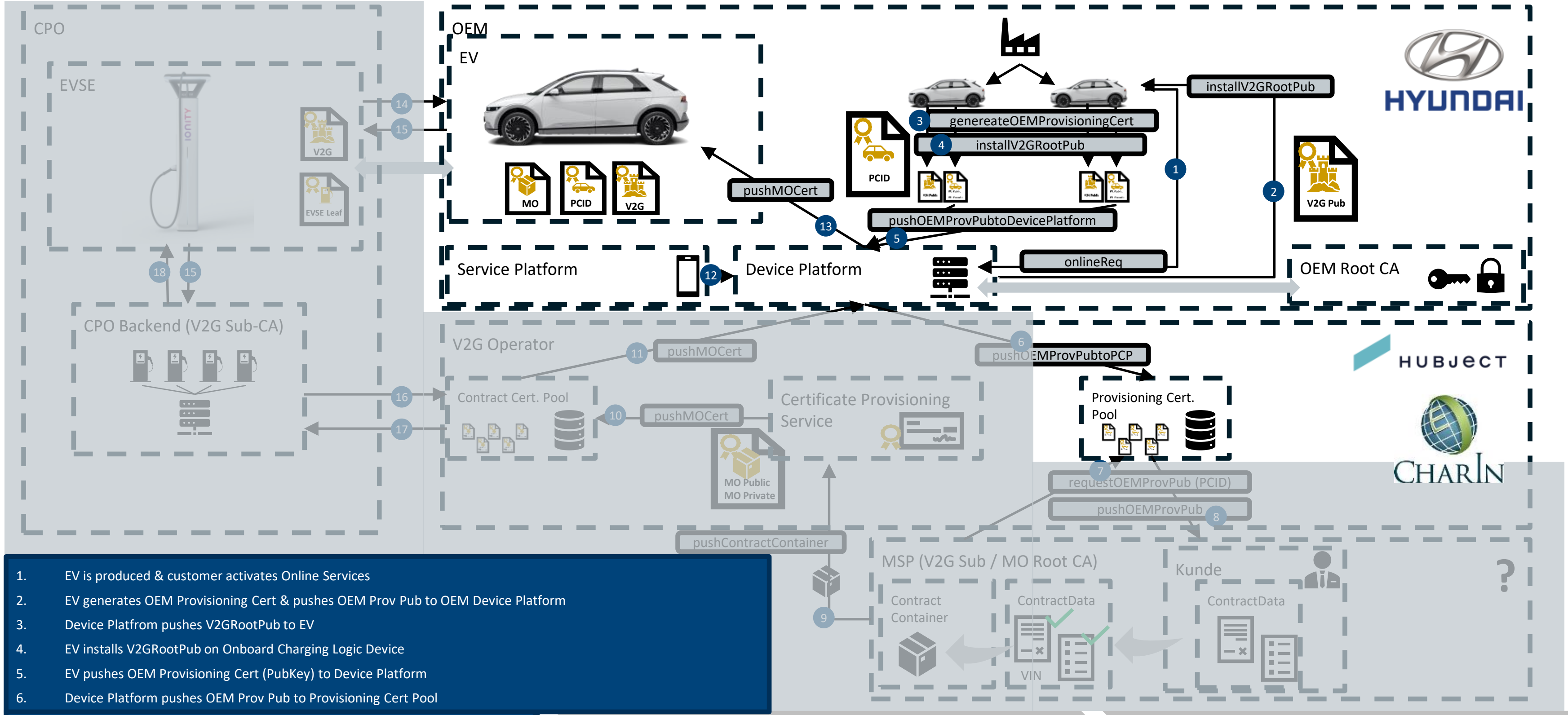
	Use Case & Application	Responsibility
PCID OEM Provisioning Certificate	▪ Proof of Identity of the EV ▪ Essential for the installation of the MO Contract Certificate (Confidentiality!)	▪ Public: OEM Provisioning Certificate Pool, MO ▪ Private: EV, Device Platform, OEM
V2G Pub V2G Root Certifificate	▪ „General Access “ for the PnC Network ▪ All entities and services have to be signed by the V2G Root CA in order to communicate to each other	▪ Public: Überall ▪ Private: Stored by V2G Root Operator
MO Vertrag MO Contract Certificate	▪ Proof of Identity for the MO Contract validity (Integrity!) ▪ Key for starting & addressing charging events ▪ Assignment of Charge Detail Records via Signature& eMAID of the MO Contract Certificate	▪ Public: Contract Certificate Pool, EV ▪ Private: MO, EV

PLUG&CHARGE PROCESS – AN OVERVIEW



Vehicle Production → Certificate Installation → Authentication

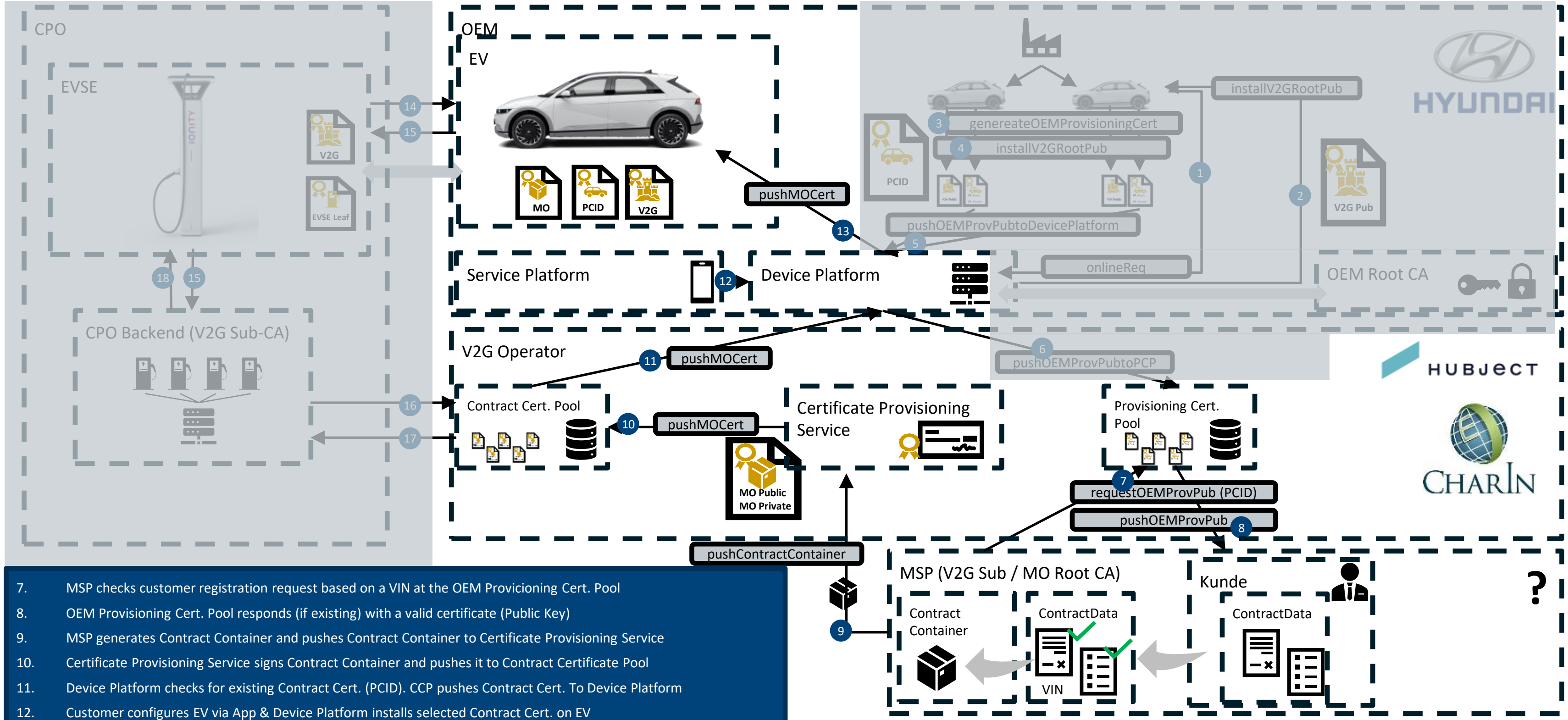
PLUG&CHARGE PROCESS – STEP 1: OEM TASKS @ VEHICLE PRODUCTION



1. EV is produced & customer activates Online Services
2. EV generates OEM Provisioning Cert & pushes OEM Prov Pub to OEM Device Platform
3. Device Platfrom pushes V2GRootPub to EV
4. EV installs V2GRootPub on Onboard Charging Logic Device
5. EV pushes OEM Provisioning Cert (PubKey) to Device Platform
6. Device Platform pushes OEM Prov Pub to Provisioning Cert Pool

Vehicle Production | Certificate Installation | Authentication

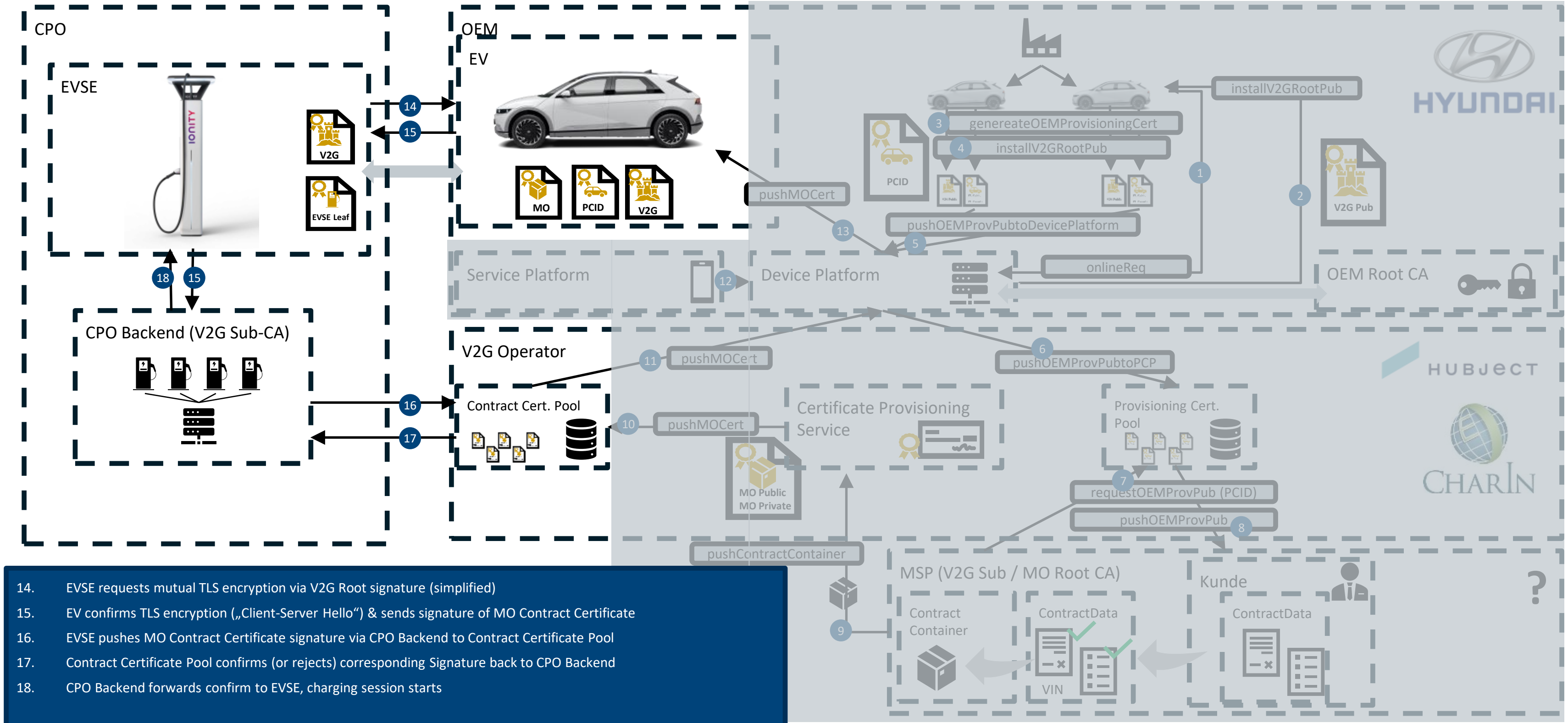
PLUG&CHARGE PROCESS – STEP 2: CONTRACT CERTIFICATE INSTALLATION



7. MSP checks customer registration request based on a VIN at the OEM Provicioning Cert. Pool
8. OEM Provisioning Cert. Pool responds (if existing) with a valid certificate (Public Key)
9. MSP generates Contract Container and pushes Contract Container to Certificate Provisioning Service
10. Certificate Provisioning Service signs Contract Container and pushes it to Contract Certificate Pool
11. Device Platform checks for existing Contract Cert. (PCID). CCP pushes Contract Cert. To Device Platform
12. Customer configures EV via App & Device Platform installs selected Contract Cert. on EV

Vehicle Production → Certificate Installation → Authentication

PLUG&CHARGE PROCESS – STEP 3: AUTHENTICATION PROCESS



14. EVSE requests mutual TLS encryption via V2G Root signature (simplified)
15. EV confirms TLS encryption („Client-Server Hello“) & sends signature of MO Contract Certificate
16. EVSE pushes MO Contract Certificate signature via CPO Backend to Contract Certificate Pool
17. Contract Certificate Pool confirms (or rejects) corresponding Signature back to CPO Backend
18. CPO Backend forwards confirm to EVSE, charging session starts

Vehicle Production → Certificate Installation → Authentication

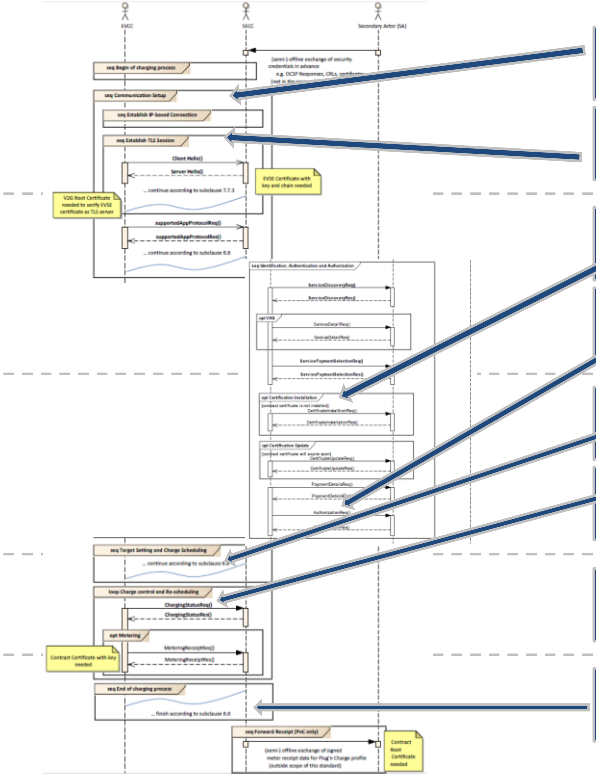
Agenda

1 **Some Basics regarding ISO 15118**

2 **ISO 15118 Structure**

- 2.1 **Begin of Charging**
- 2.2 **TLS Session Setup**
- 2.3 **Session Setup and Services**
- 2.4 **Certificate Handling**
- 2.5 **Charging Procedure**

3 **Not described within ISO 15118 but required**


EVCC
SECC
Secondary Actor (SA)
(semi-) offline exchange of security credentials in advance
e.g. OCSP Responses, CRLs, certificates
(not in the scope of ...
seq Begin of charging process
seq Communication Setup
seq Establish IP-based Connection
seq Establish TLS Session
Client Hello()
Server Hello()
... continue according to subclause 7.7.3
EVSE Certificate with key and chain needed
V2G Root Certificate needed to verify EVSE certificate as TLS server
supportedAppProtocolReq()
supportedAppProtocolRes()
... continue according to subclause 8.8
seq Identification, Authentication and Authorization
ServiceDiscoveryReq()
ServiceDiscoveryRes()
opt VAS
ServiceDetailReq()
ServiceDetailRes()
ServicePaymentSelectionReq()
ServicePaymentSelectionRes()
opt Certification Installation
[contract certificate is not installed]
CertificateInstallationReq()
CertificateInstallationRes()
opt Certification Update
[contract certificate will expire soon]
CertificateUpdateReq()
CertificateUpdateRes()
PaymentDetailsReq()
PaymentDetailsRes()
AuthorizationReq()
seq Target Setting and Charge Scheduling
... continue according to subclause 8.8
loop Charge control and Re-scheduling
ChargingStatusReq()
ChargingStatusRes()
opt Metering
MeteringReceiptReq()
MeteringReceiptRes()
Contract Certificate with key needed
seq End of charging process
... finish according to subclause 8.8
seq Forward Receipt (PnC only)
(semi-) offline exchange of signed meter receipt data for Plug'n Charge profile (outside scope of this standard)
Contract Root Certificate needed

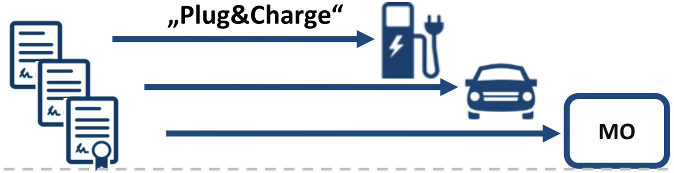
A Start of Charging Process

B Communication Setup

Request
Response

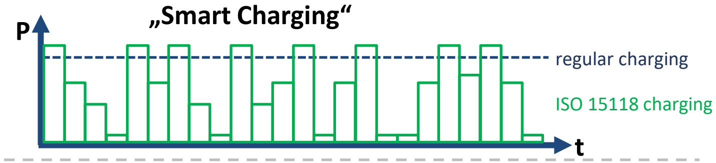
C Certificate Handling

D Identification, Authentication and Authorization



E Target Setting and charge scheduling

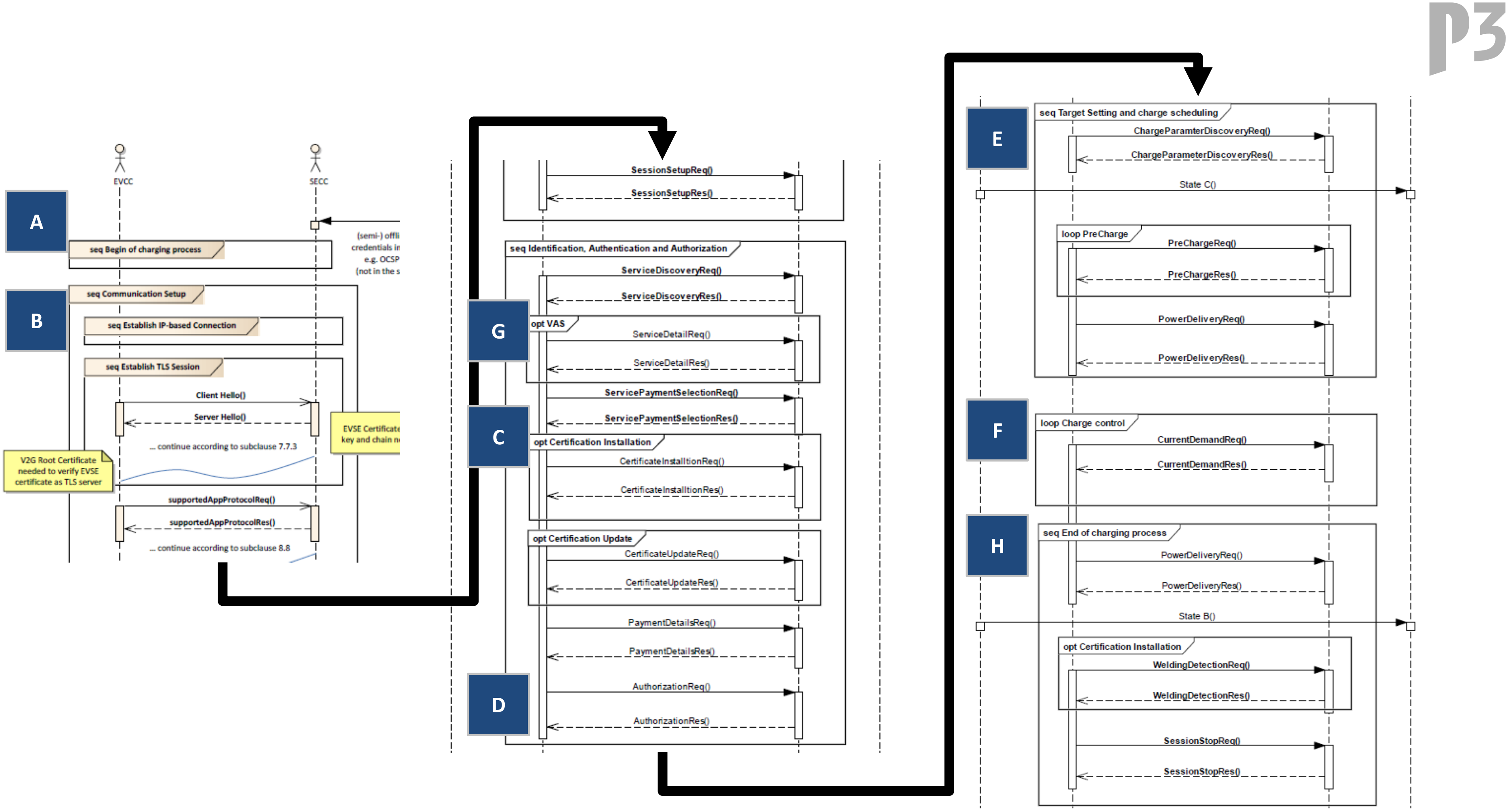
F Charge Controlling and Re-Scheduling



G Value Added Services

● Charging ● Additional Charging Services ● Vehicle Services ● Location Based Services

H End of Charging Process



P3

EVCC

SECC

A

seq Begin of charging process

(semi-) offli
credentials in
e.g. OCSP
(not in the s

B

seq Communication Setup

seq Establish IP-based Connection

seq Establish TLS Session

Client Hello()

Server Hello()

EVSE Certificate
key and chain n

... continue according to subclause 7.7.3

V2G Root Certificate
needed to verify EVSE
certificate as TLS server

supportedAppProtocolReq()

supportedAppProtocolRes()

... continue according to subclause 8.8

SessionSetupReq()

SessionSetupRes()

seq Identification, Authentication and Authorization

ServiceDiscoveryReq()

ServiceDiscoveryRes()

G

opt VAS

ServiceDetailReq()

ServiceDetailRes()

ServicePaymentSelectionReq()

ServicePaymentSelectionRes()

C

opt Certification Installation

CertificateInstalltionReq()

CertificateInstalltionRes()

opt Certification Update

CertificateUpdateReq()

CertificateUpdateRes()

PaymentDetailsReq()

PaymentDetailsRes()

D

AuthorizationReq()

AuthorizationRes()

E

seq Target Setting and charge scheduling

ChargeParamterDiscoveryReq()

ChargeParameterDiscoveryRes()

State C()

loop PreCharge

PreChargeReq()

PreChargeRes()

PowerDeliveryReq()

PowerDeliveryRes()

F

loop Charge control

CurrentDemandReq()

CurrentDemandRes()

H

seq End of charging process

PowerDeliveryReq()

PowerDeliveryRes()

State B()

opt Certification Installation

WeldingDetectionReq()

WeldingDetectionRes()

SessionStopReq()

SessionStopRes()

Agenda

1 Some Basics regarding ISO 15118

2 ISO 15118 Structure

2.1 **Begin of Charging**

2.2 TLS Session Setup

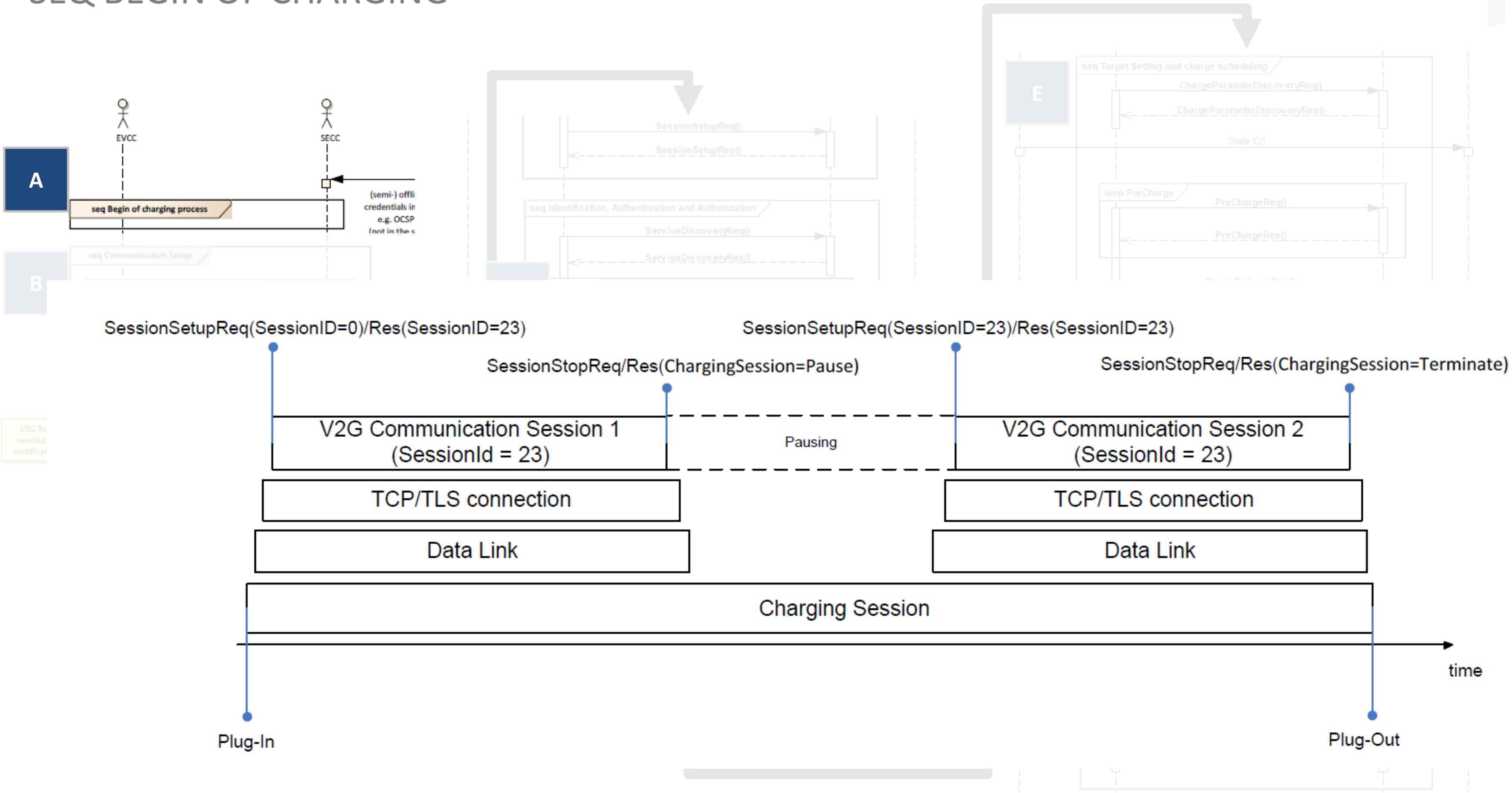
2.3 Session Setup and Services

2.4 Certificate Handling

2.5 Charging Procedure

3 Not described within ISO 15118 but required

SEQ BEGIN OF CHARGING



SessionSetupReq(SessionID=0)/Res(SessionID=23)

SessionStopReq/Res(ChargingSession=Pause)

SessionSetupReq(SessionID=23)/Res(SessionID=23)

SessionStopReq/Res(ChargingSession=Terminate)

V2G Communication Session 1 (SessionId = 23)

Pausing

V2G Communication Session 2 (SessionId = 23)

TCP/TLS connection

TCP/TLS connection

Data Link

Data Link

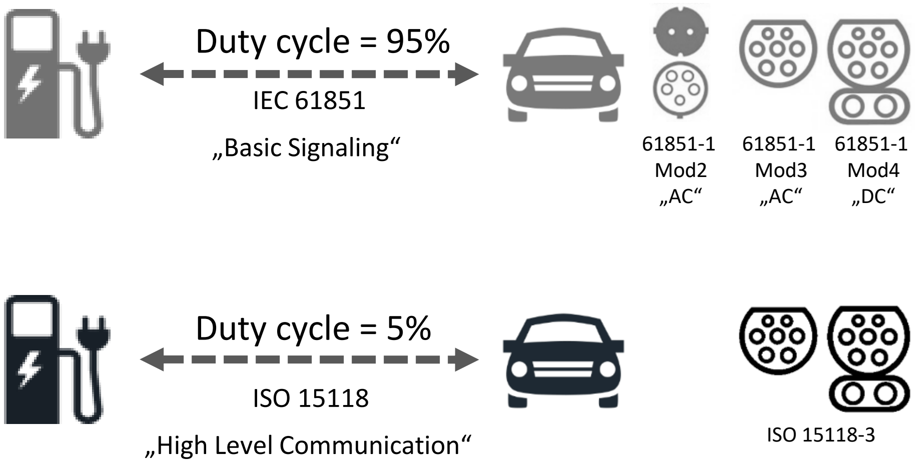
Charging Session

time

Plug-In

Plug-Out

Depending on the duty cycle , EV and EVSE differ between „Basic Signaling“ (IEC 61851) and „High Level Communication“



Duty cycle = 95%

IEC 61851

„Basic Signaling“

61851-1 Mod2 „AC“

61851-1 Mod3 „AC“

61851-1 Mod4 „DC“

Duty cycle = 5%

ISO 15118

„High Level Communication“

ISO 15118-3

IEC 61851 (2010)

- 4 charging modes (a, b, c, d)
- Communication initated by EVSE
- Charging information exchanged via PWM signals

ISO 15118 (Edition 1.0 von 2014, Edition 2.0 in 2019)

- 2 Charging modes (AC/DC)
- 2 Authentication modes (EIM/PnC)
- Communication initiated via EV
- Charging information exchanged via PLC signals
- Negitiation of „Charging Parameters“ always initiated by EV

Agenda

1 Some Basics regarding ISO 15118

2 ISO 15118 Structure

2.1 Begin of Charging

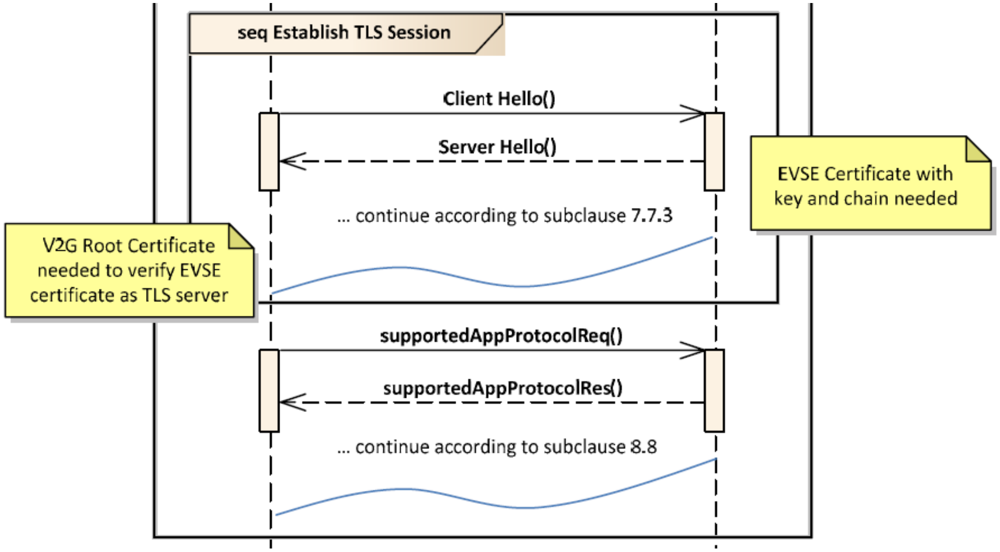
2.2 TLS Session Setup

2.3 Session Setup and Services

2.4 Certificate Handling

2.5 Charging Procedure

3 Not described within ISO 15118 but requ

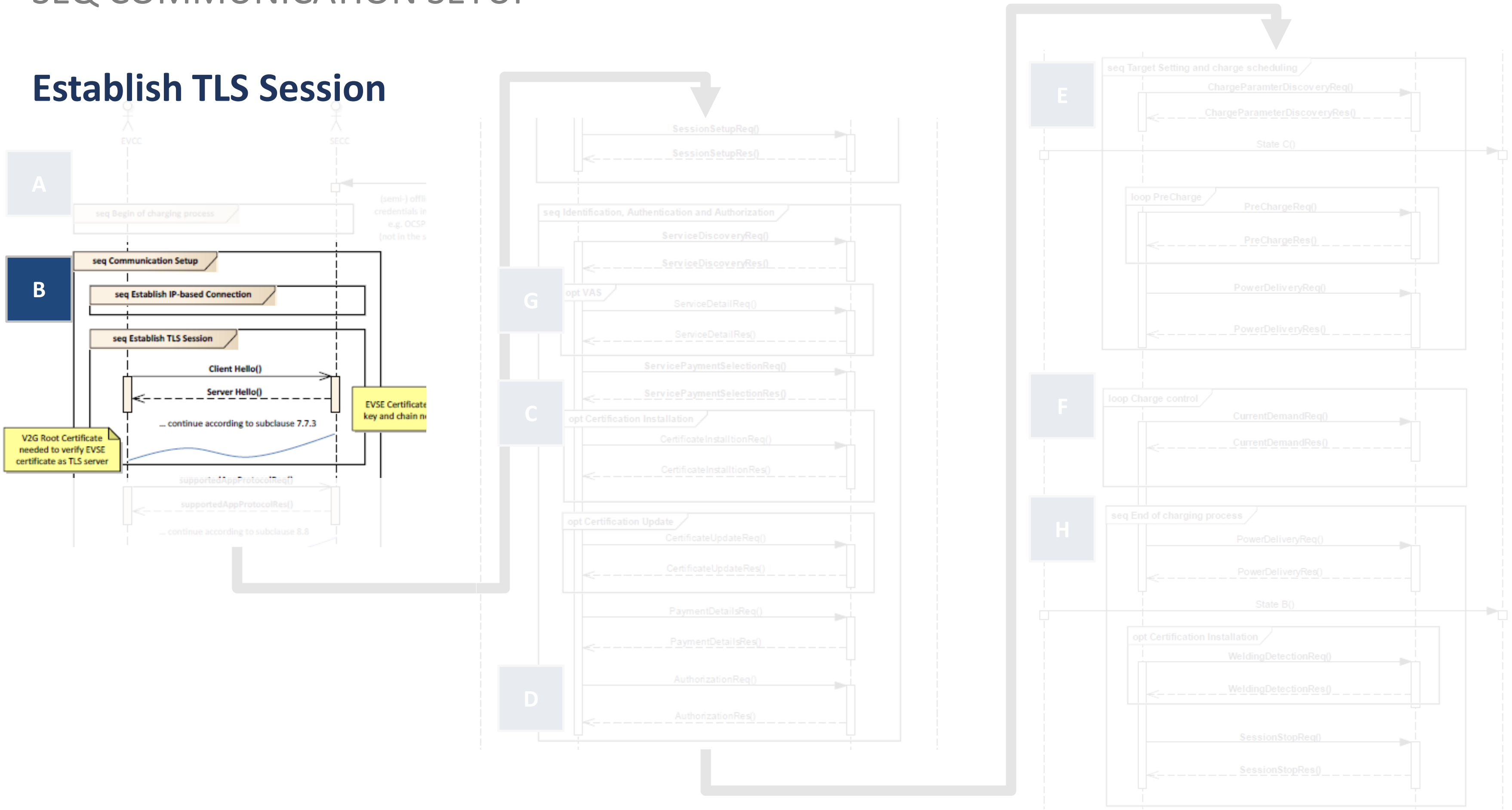

seq Establish TLS Session
Client Hello()
Server Hello()
... continue according to subclause 7.7.3
supportedAppProtocolReq()
supportedAppProtocolRes()
... continue according to subclause 8.8

EVSE Certificate with key and chain needed

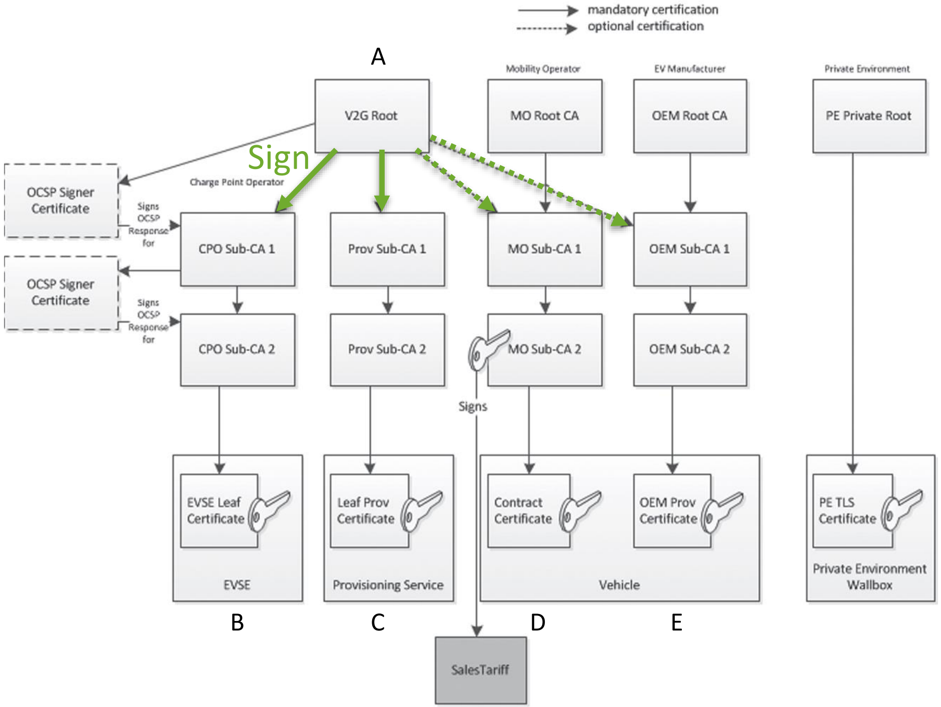
V2G Root Certificate needed to verify EVSE certificate as TLS server

SEQ COMMUNICATION SETUP

Establish TLS Session

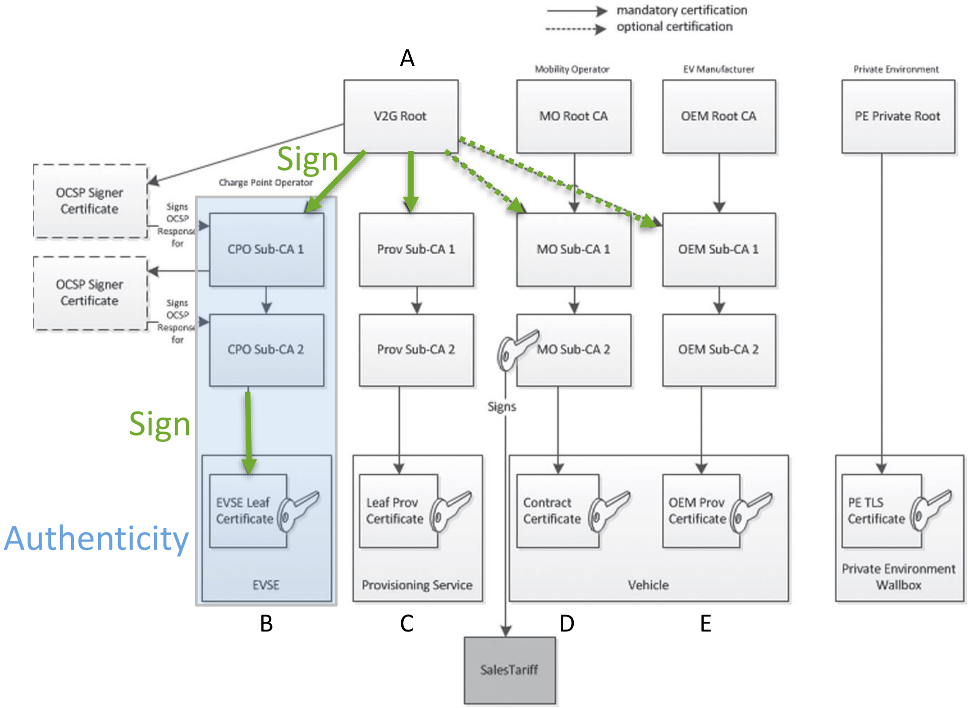


TLS Session Setup – Certificate Handling



a) A trusted authority provides and manages the V2G Root certificate. This authority signs underlaying Sub-CA certificates for infrastructure partners as CPO’s, provisioning serivces, MO’s and OEM’s (MO’s and OEM’s are optional).

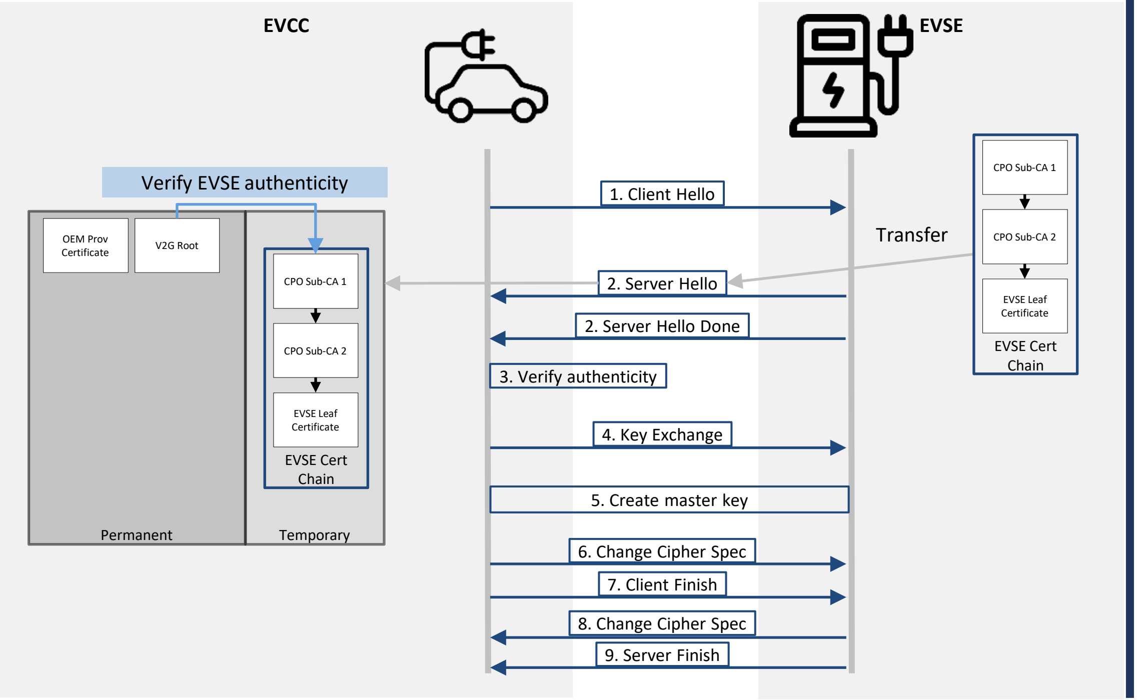
TLS Session Setup – Certificate Handling



a) A trusted authority provides and manages the V2G Root certificate. This authority signs underlaying Sub-CA certificates for infrastructure partners as CPO’s, provisioning serivces, MO’s and OEM’s (MO’s and OEM’s are optional).

b) The EVSE Leaf certificate is created for each EVSE and signed by an authority above. The authenticity of the EVSE can be verified with the EVSE Leaf certificate chain. That is done by the EVCC for the TLS handshake.

The TLS Session is established via definition of IETF RFC 6066 and follows the standard TLS procedure



Working Principle of Client/Server Hello

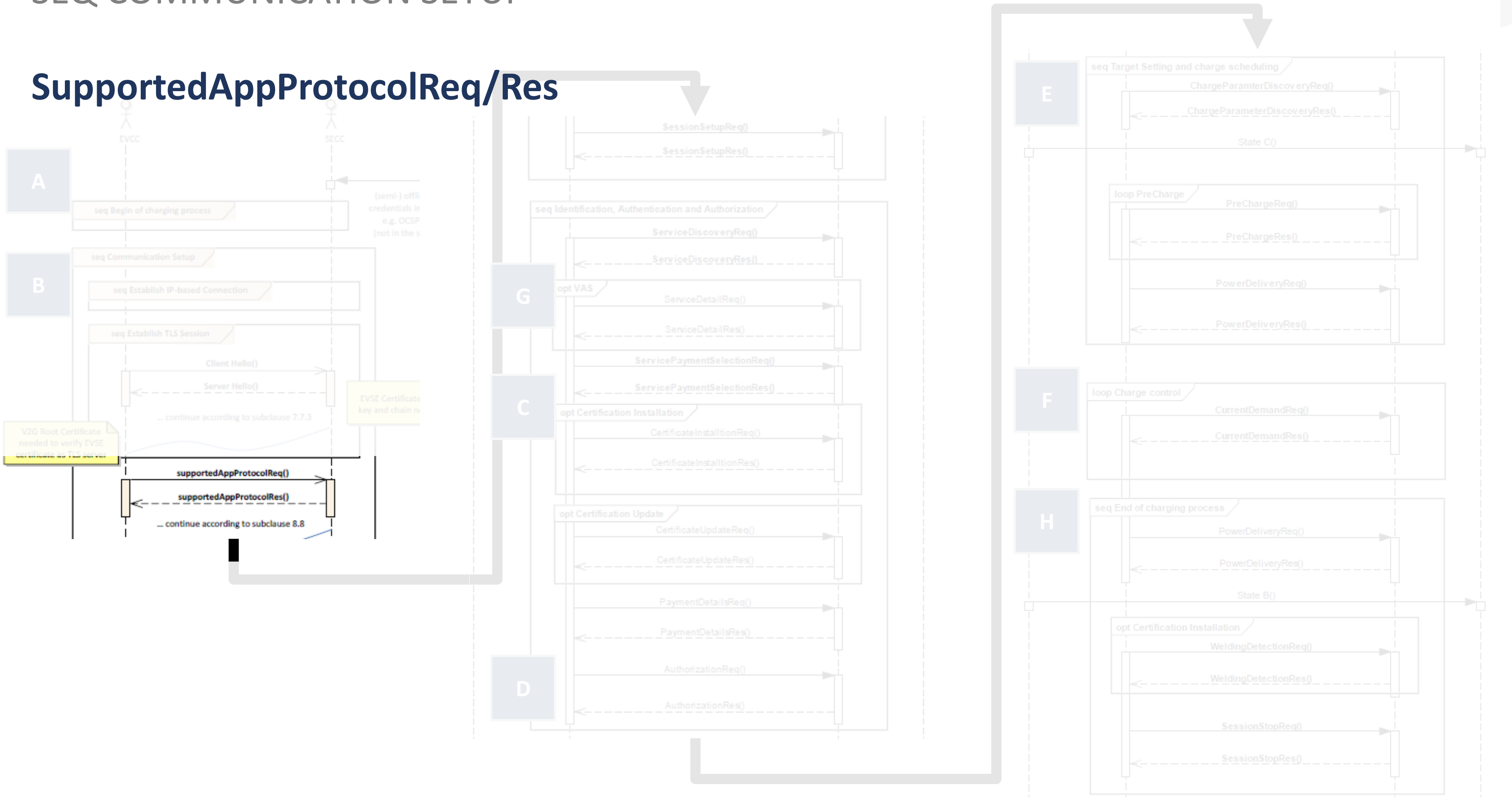
- Client/Server Hello according to TLS Handshake
- Definition in IETF RFC 6066
- https://tools.ietf.org/html/rfc6066

Sequence

1. After connecting the cable, the EVCC (Client) sends Client Hello including a random number
2. The EVSE (Server) replies Server Hello with it‘s Leaf certificate chain and a random number(Server Hello), followed by Server Hello Done
3. EVCC authenticates EVSE Leaf by matching signatures with stored V2G Root certificate to know the EVSE can be trusted
4. The EVCC creates a pre-mastered key, encrypts it with the EVSE Leaf Certificate and sends it to the EVSE with Key Exchange.
5. The EVCC and the EVSE create a master key for the TLS session with the pre-mastered key and the random number they send each other.
6. 7./8./9. With the Change Cipher Spec and Client/Server Finish message, both parties switch to encrypted communication.

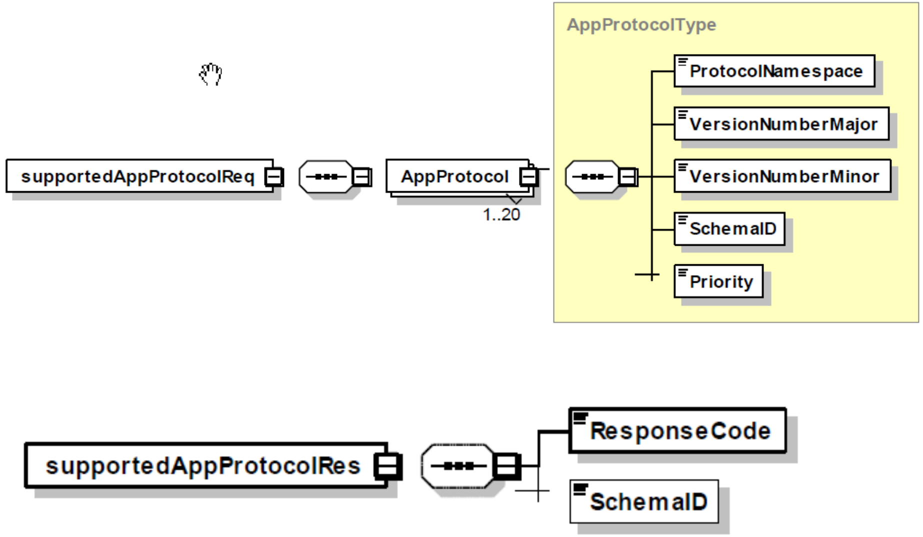
SEQ COMMUNICATION SETUP

SupportedAppProtocolReq/Res



SupportedAppProtocolReq/Res

Message Schema Diagram of supportedAppProtocolReq /Res



Description

- **This message pair provides additional information between EVCC and SECC about the used versions of ISO 15118**
- **With the matching of protocol versions, interoperability is increased and miss-communication avoided**
- **This message becomes more important with multiple ISO 15118 versions released**

Agenda

1 **Some Basics regarding ISO 15118**

2 **ISO 15118 Structure**

2.1 **Begin of Charging**

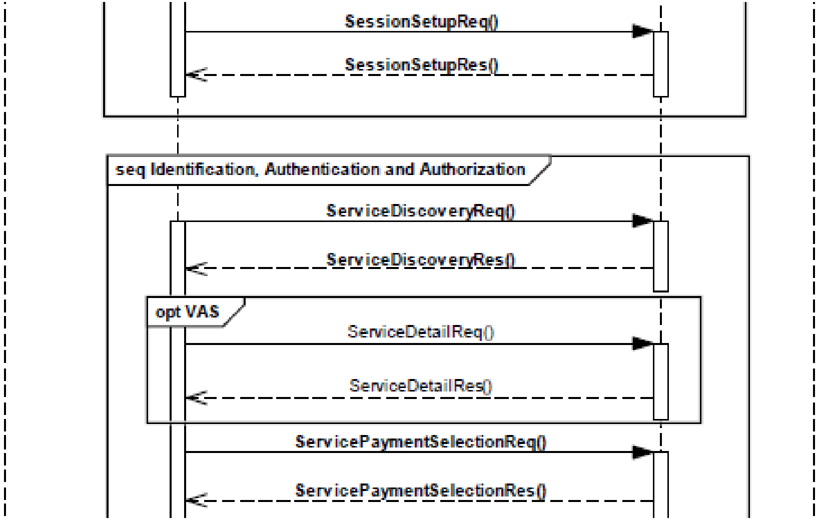
2.2 **TLS Session Setup**

2.3 **Session Setup and Services**

2.4 **Certificate Handling**

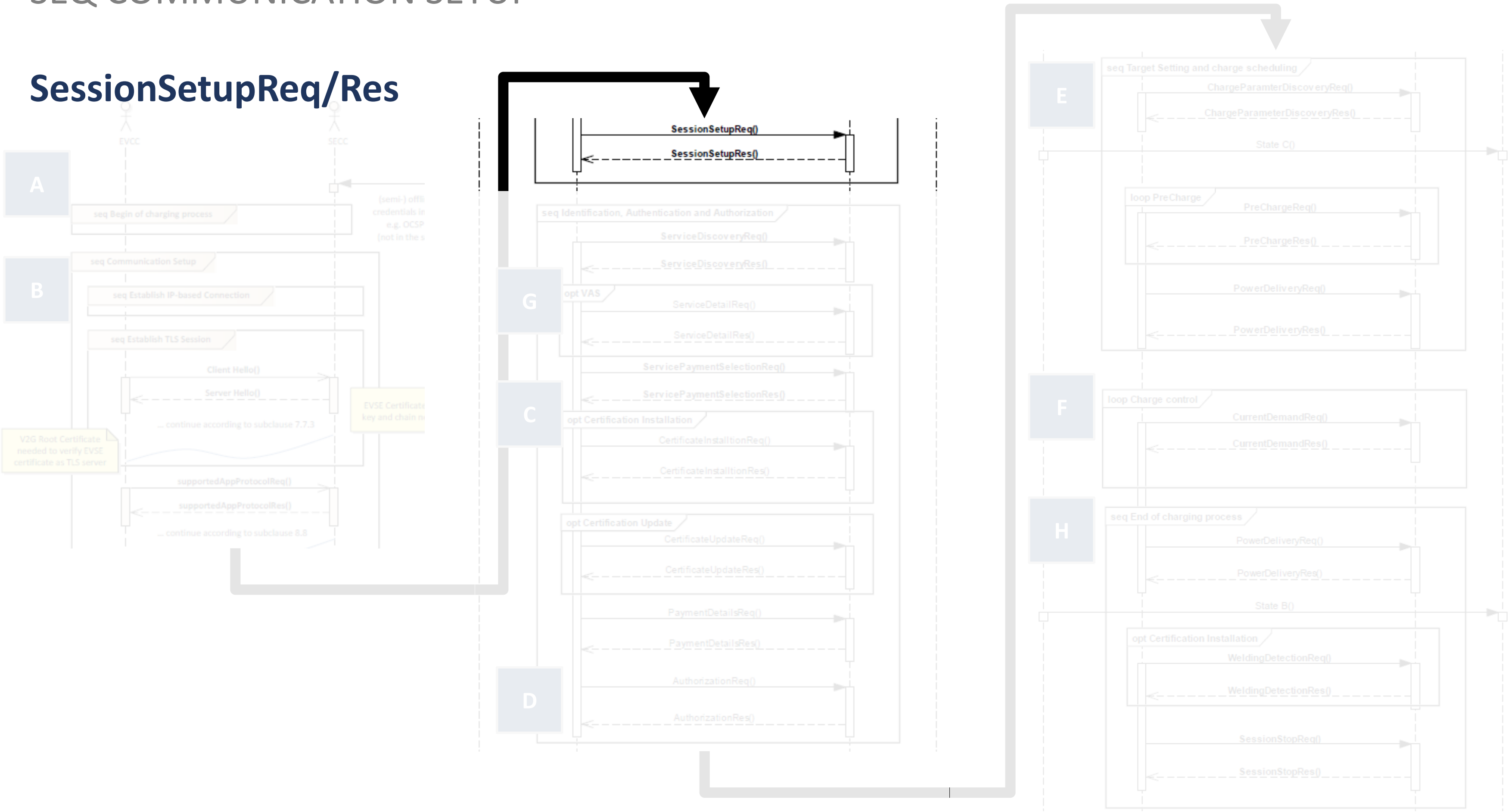
2.5 **Charging Procedure**

3 **Not described within ISO 15118 but required**



SEQ COMMUNICATION SETUP

SessionSetupReq/Res

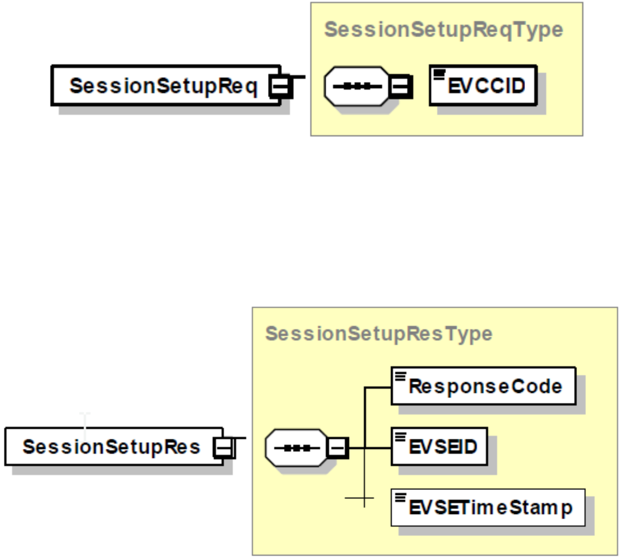


SessionSetupReq/Res

Working Principle of Session Setup

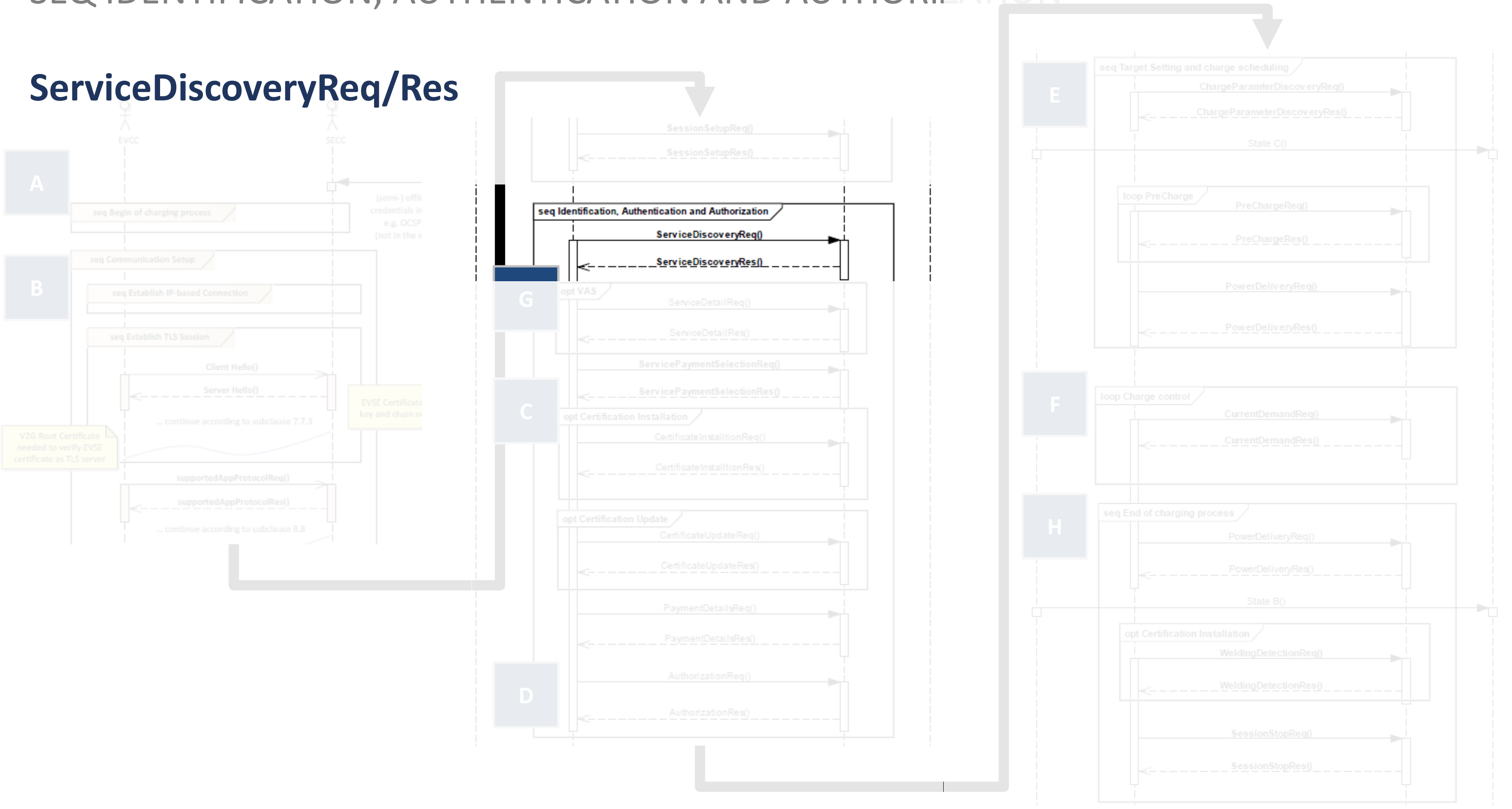
- By using the SessionSetupReq message the EVCC establishes a V2G communication session
- EVCC initiates communication by sending the EVCCID (mac address) to the SECC
- SECC acknowledges with a response code, the EVSEID and a timestamp

Schema



SEQ IDENTIFICATION, AUTHENTICATION AND AUTHORIZATION

ServiceDiscoveryReq/Res

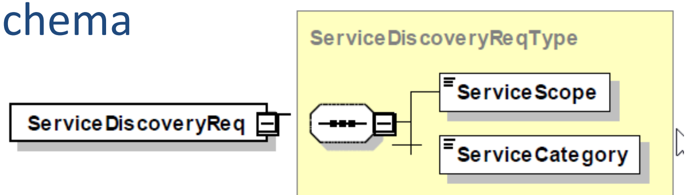


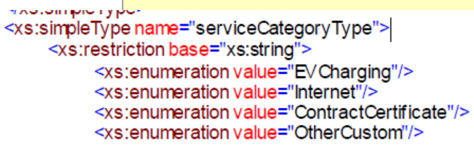
ServiceDiscoveryReq/Res

Working Principle of ServiceDiscoveryReq/Res

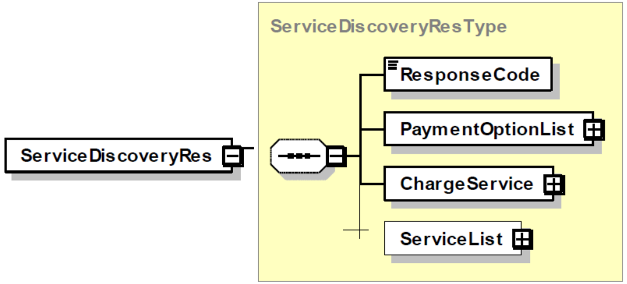
- **With this message pair, SECC provides EVCC with all available services of the EVSE.**
- **ServiceCategoryTypes offers EV Charging, Internet and ContractCertificate. Additionally, customized services can be added (but require definition on both sides, EV and EVSE)**

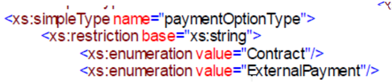
Schema



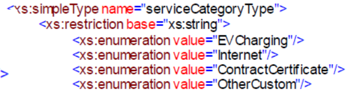


```
<xs:simpleType name="serviceCategoryType">
    <xs:restriction base="xs:string">
        <xs:enumeration value="EVCharging"/>
        <xs:enumeration value="Internet"/>
        <xs:enumeration value="ContractCertificate"/>
        <xs:enumeration value="OtherCustom"/>
```





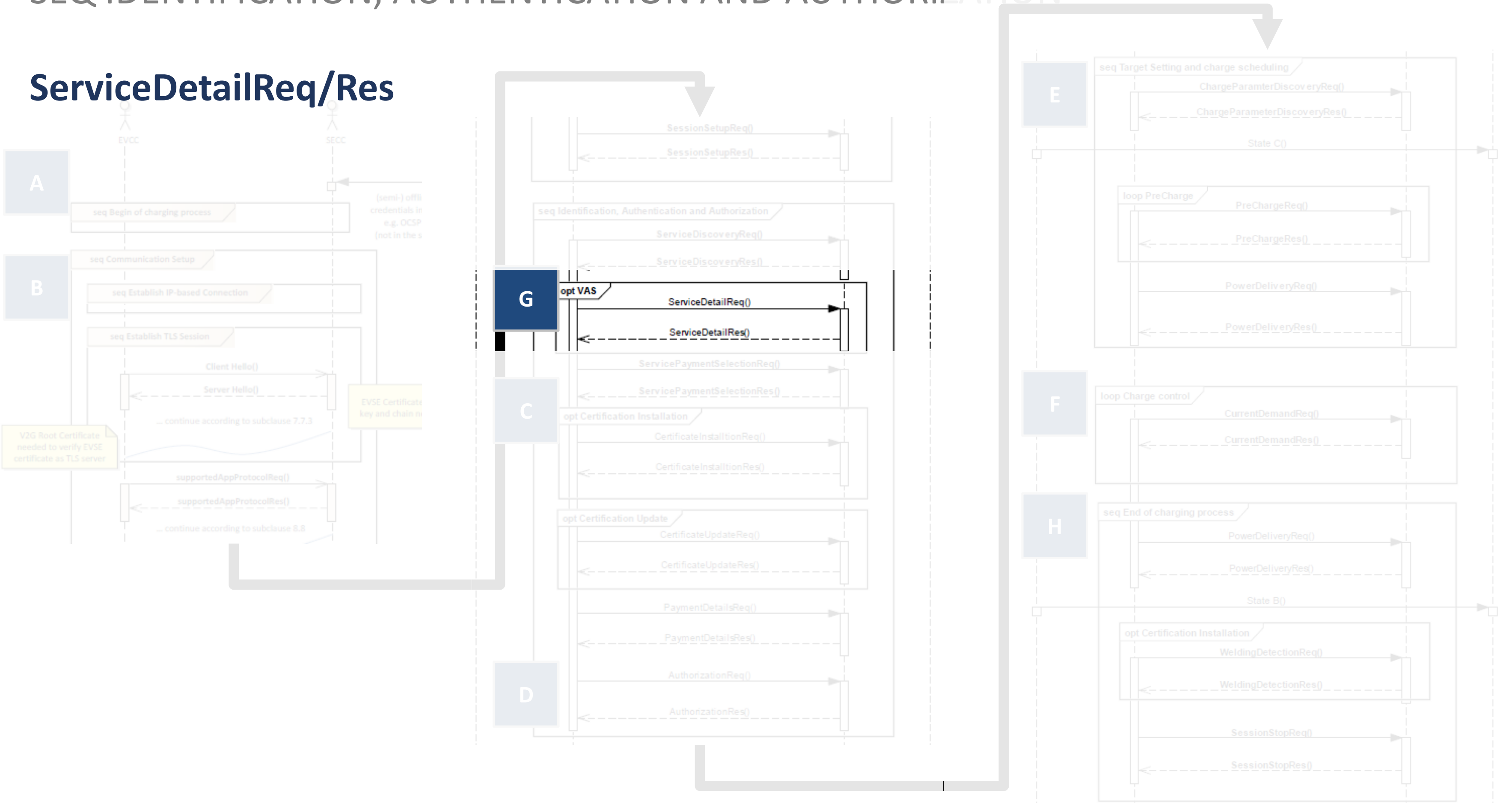
```
<xs:simpleType name="paymentOptionType">
    <xs:restriction base="xs:string">
        <xs:enumeration value="Contract"/>
        <xs:enumeration value="ExternalPayment"/>
```



```
<xs:simpleType name="serviceCategoryType">
    <xs:restriction base="xs:string">
        <xs:enumeration value="EVCharging"/>
        <xs:enumeration value="Internet"/>
        <xs:enumeration value="ContractCertificate"/>
        <xs:enumeration value="OtherCustom"/>
```

SEQ IDENTIFICATION, AUTHENTICATION AND AUTHORIZATION

ServiceDetailReq/Res

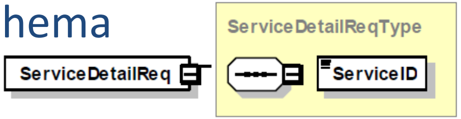


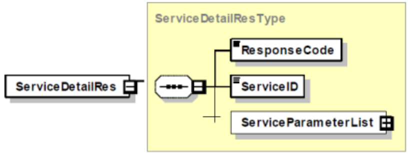
ServiceDetailReq/Res

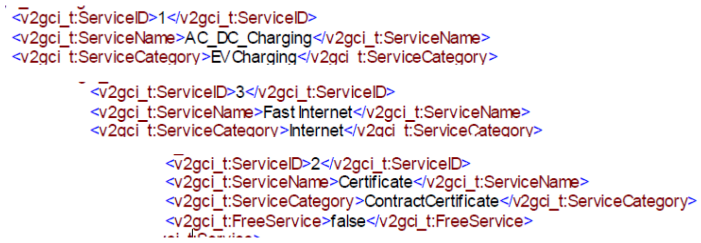
Working Principle of ServiceDetailReq/Res

- **EVCC requests further service options from SECC.**
- **SECC confirms service request (ResponseCode) and sends available services at EVSE to EV.**
- **Available EVSE services are clustered in charging mode (AC/DC), certificate installation availability, internet access and further non-specified options (place holders)**
- **Charging modes, certificate installation and internet option are the most important serviceids**

Schema





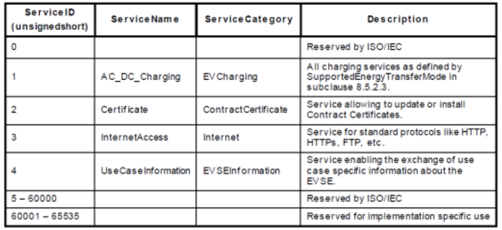


```
<v2gci_t:ServiceID>1</v2gci_t:ServiceID>
<v2gci_t:ServiceName>AC_DC_Charging</v2gci_t:ServiceName>
<v2gci_t:ServiceCategory>EVCharging</v2gci_t:ServiceCategory>

    <v2gci_t:ServiceID>3</v2gci_t:ServiceID>
    <v2gci_t:ServiceName>Fast Internet</v2gci_t:ServiceName>
    <v2gci_t:ServiceCategory>Internet</v2gci_t:ServiceCategory>

        <v2gci_t:ServiceID>2</v2gci_t:ServiceID>
        <v2gci_t:ServiceName>Certificate</v2gci_t:ServiceName>
        <v2gci_t:ServiceCategory>ContractCertificate</v2gci_t:ServiceCategory>
        <v2gci_t:FreeService>false</v2gci_t:FreeService>
```

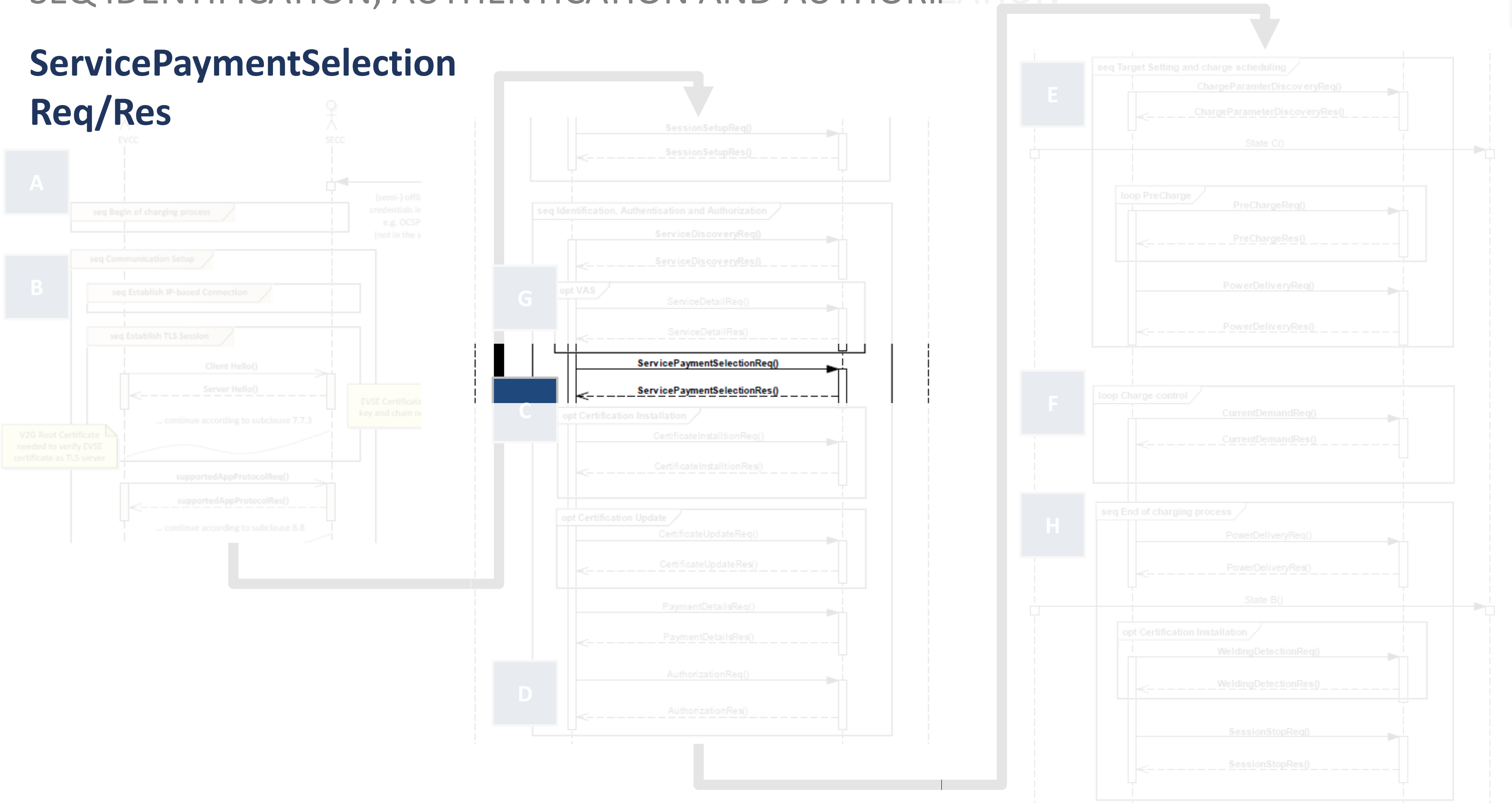
Table 105 — Definition of ServiceID, Service Category, Service Name, and Service Scope



ServiceID (unsignedshort)	ServiceName	ServiceCategory	Description
0			Reserved by ISO/IEC
1	AC_DC_Charging	EVCharging	All charging services as defined by SupportedEnergyTransferMode in subclause 8.5.2.3.
2	Certificate	ContractCertificate	Service allowing to update or install Contract Certificates.
3	InternetAccess	Internet	Service for standard protocols like HTTP, HTTPs, FTP, etc.
4	UseCaseInformation	EVSEInformation	Service enabling the exchange of use case specific information about the EVSE.
5 – 60000			Reserved by ISO/IEC
60001 – 65535			Reserved for implementation specific use

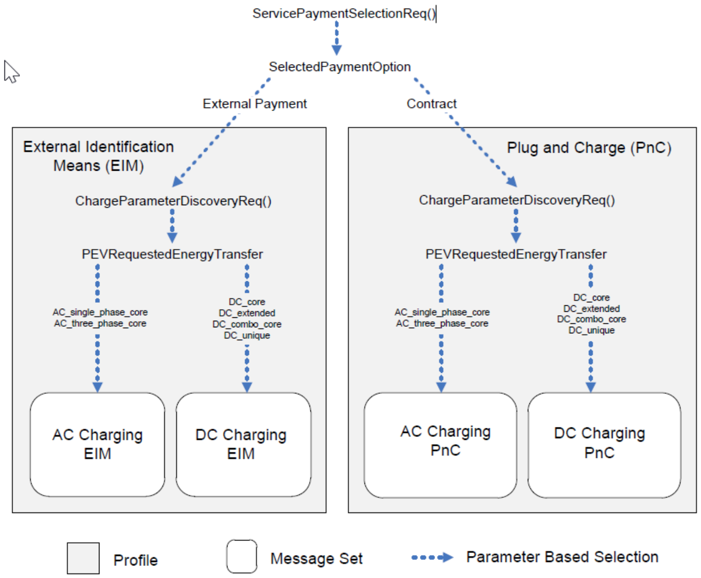
SEQ IDENTIFICATION, AUTHENTICATION AND AUTHORIZATION

ServicePaymentSelection Req/Res



ServicePaymentSelectionReq/Res

Schema of ServicePaymentSelectionReq



Description

- **ServiceParameterSelectionReq is a state machine which determines further message sets.**
- **Destinction between 4 payment modes:**
  - **AC or DC via External Identification Means**
  - **AC or DC via Plug&Charge (Certificates)**
- **Depending on the selection, it is chosen between 4 different message sets. EIM and PnC message sets are common for the largest part however charging modes differ (AC/DC)**

Agenda

1 **Some Basics regarding ISO 15118**

2 **ISO 15118 Structure**

2.1 **Begin of Charging**

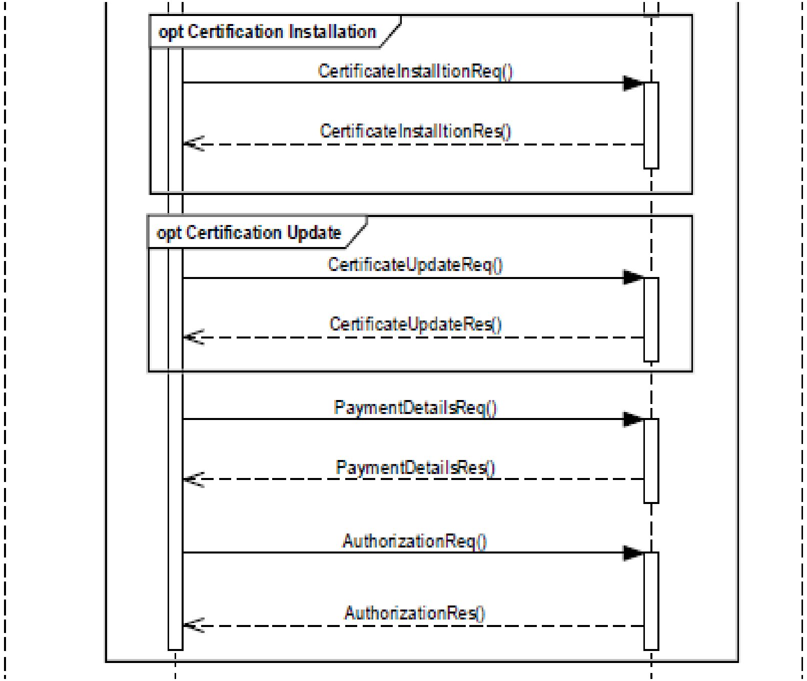
2.2 **TLS Session Setup**

2.3 **Session Setup and Services**

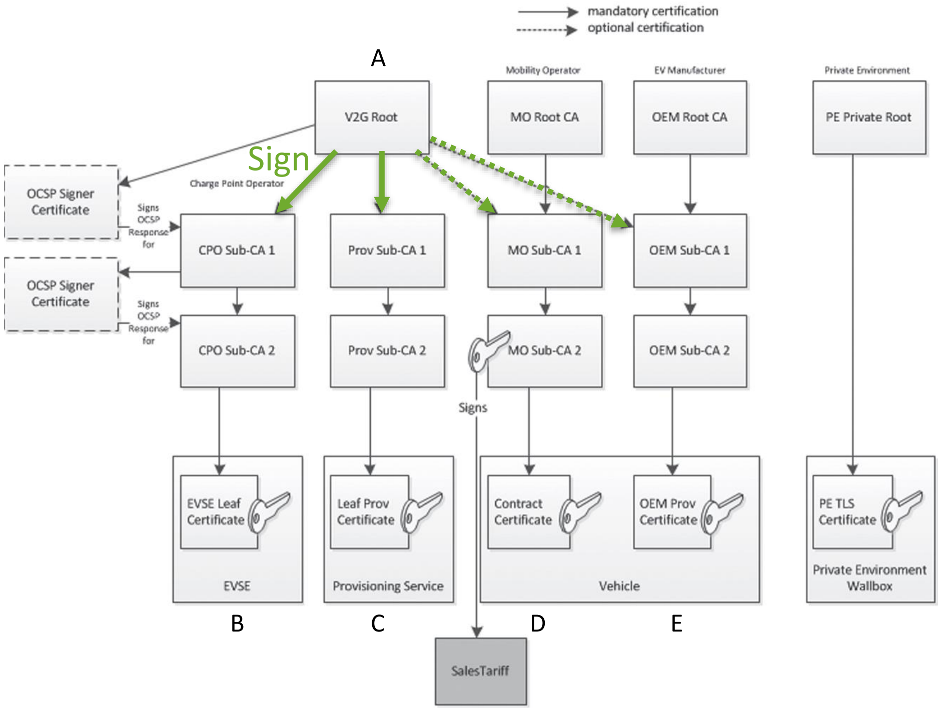
2.4 **Certificate Handling**

2.5 **Charging Procedure**

3 **Not described within ISO 15118 but required**

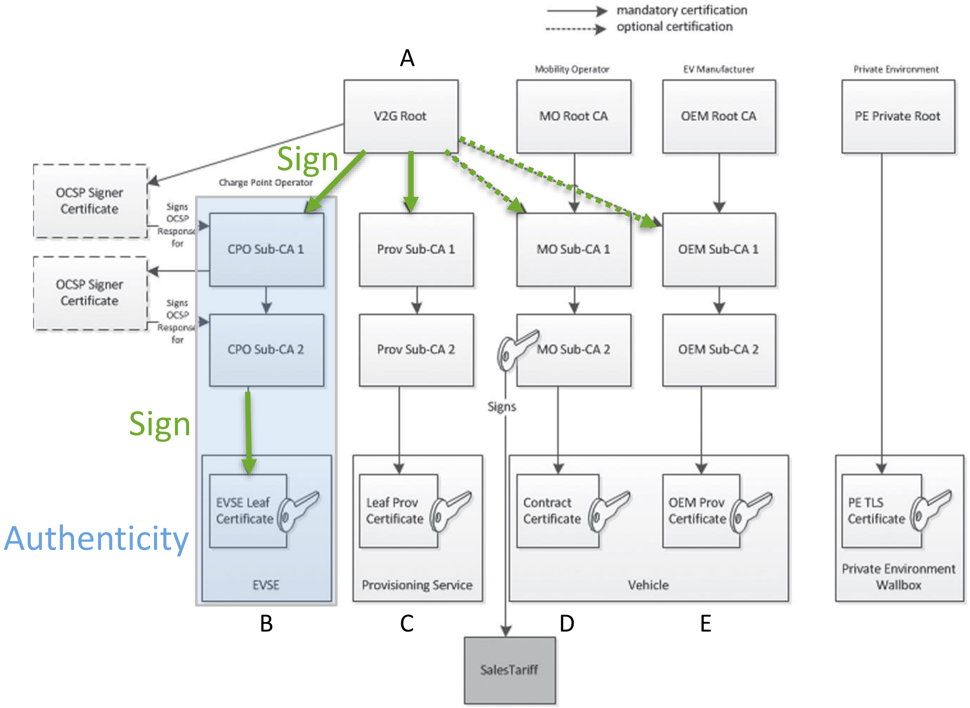


Certificate Handling - Overview



a) A trusted authority provides and manages the V2G Root certificate. This authority signs underlaying Sub-CA certificates for infrastructure partners as CPO’s, provisioning serivces, MO’s and OEM’s (MO’s and OEM’s are optional).

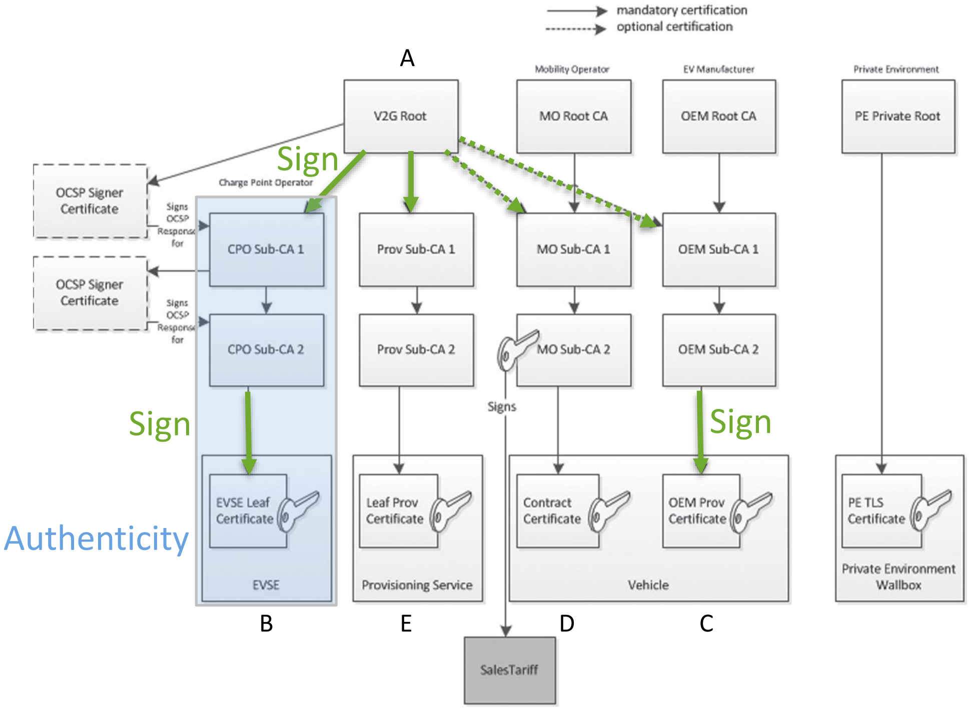
Certificate Handling - Overview



a) A trusted authority provides and manages the V2G Root certificate. This authority signs underlaying Sub-CA certificates for infrastructure partners as CPO’s, provisioning serivces, MO’s and OEM’s (MO’s and OEM’s are optional).

b) The EVSE Leaf certificate is created for each EVSE and signed by an authority above. The authenticity of the EVSE can be verified with the EVSE Leaf certificate chain. That is done by the EVCC for the TLS handshake.

Certificate Handling - Overview

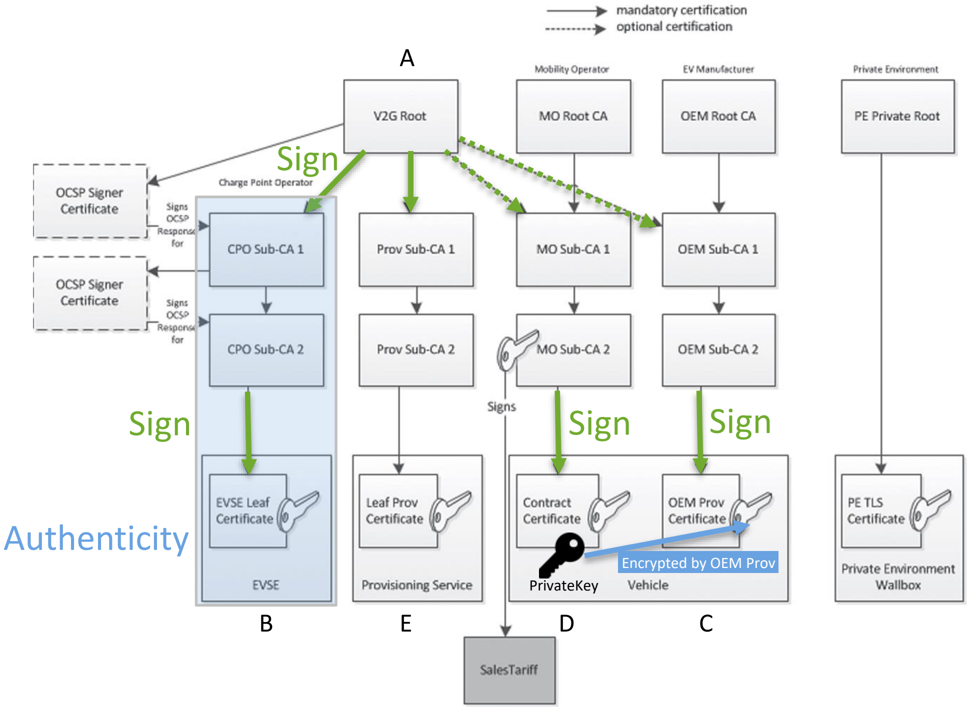


a) A trusted authority provides and manages the V2G Root certificate. This authority signs underlaying Sub-CA certificates for infrastructure partners as CPO’s, provisioning serivces, MO’s and OEM’s (MO’s and OEM’s are optional).

b) The EVSE Leaf certificate is created for each EVSE and signed by the CPO Sub-CA. The authenticity of the EVSE can be verified with the EVSE Leaf certificate chain.

c) The OEM Prov certificate is created and signed by the OEM or V2G root. Each OEM Prov certificate identifies at least a customer or the vehicle of the customer. With the OEM Prov certificate and its underlaying PCID, the customer/vehicle can be identified within the certificate infrastructure.

Certificate Handling - Overview



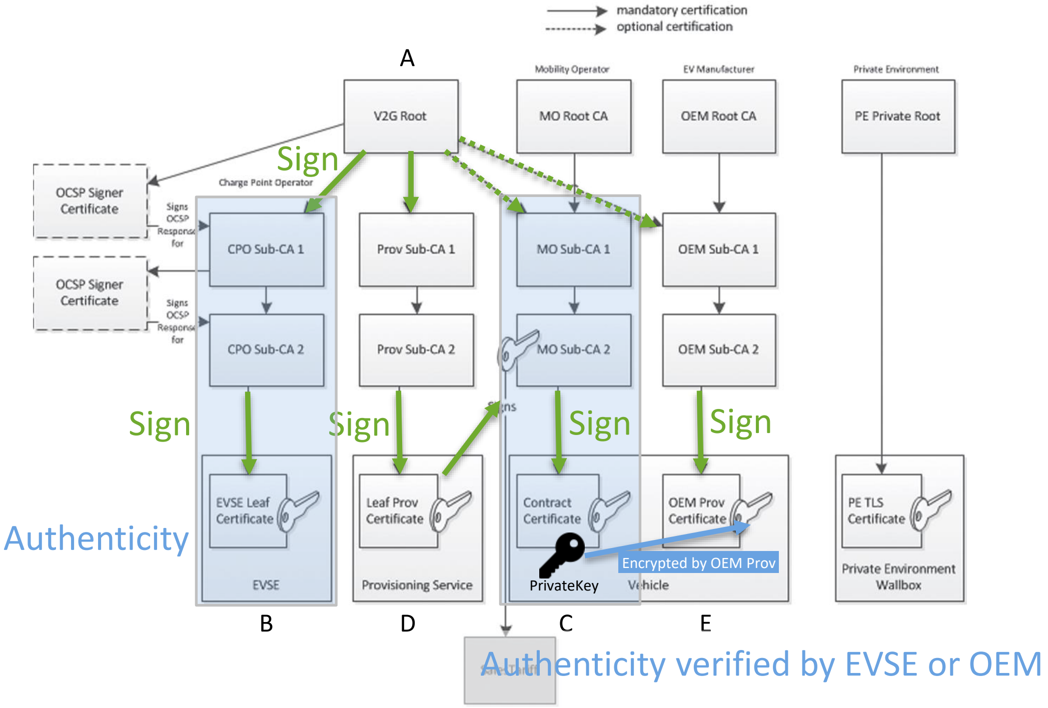
a) A trusted authority provides and manages the V2G Root certificate. This authority signs underlaying Sub-CA certificates for infrastructure partners as CPO's, provisioning serivces, MO's and OEM's (MO's and OEM's are optional).

b) The EVSE Leaf certificate is created for each EVSE and signed by the CPO. The authenticity of the EVSE can be verified with the EVSE Leaf certificate chain.

c) The OEM Prov certificate is created and signed by the OEM. Each OEM Prov certificate identifies at least a customer or the vehicle of the customer. With the OEM Prov certificate and its underlaying PCID, the customer/vehicle can be identified within the certificate infrastructure.

d) The Contract certificate is created and signed by the MO or V2G root. The MO needs the PCID for the creation because the private key of the contract certificate will be encrypted by the OEM Prov certificate.

Certificate Handling - Overview



a) A trusted authority provides and manages the V2G Root certificate. This authority signs underlaying Sub-CA certificates for infrastructure partners as CPO's, provisioning serivces, MO's and OEM's (MO's and OEM's are optional).

b) The EVSE Leaf certificate is created for each EVSE and signed by the CPO Sub-CA. The authenticity of the EVSE can be verified with the EVSE Leaf certificate chain.

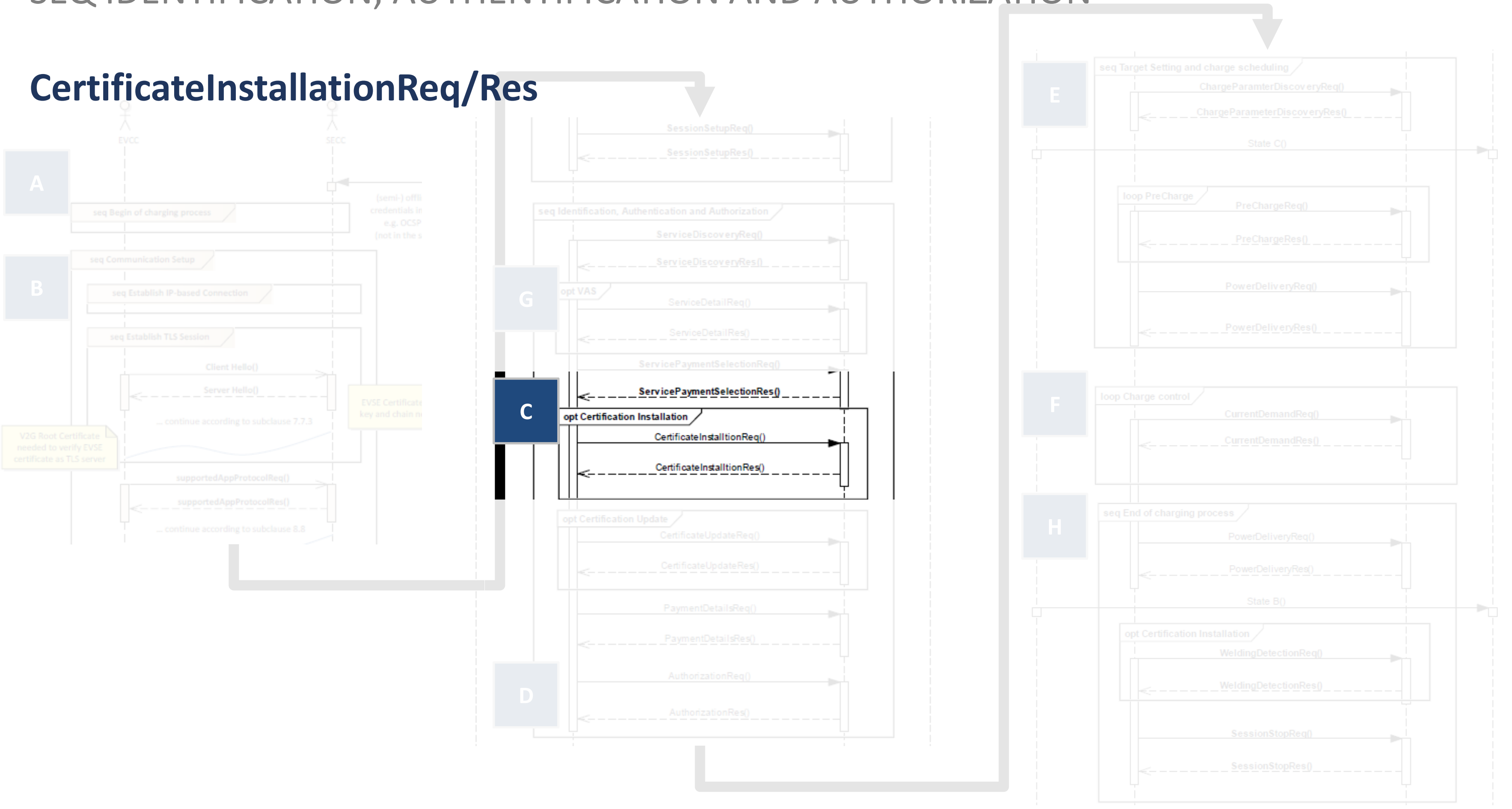
c) The OEM Prov certificate is created and signed by the OEM. Each OEM Prov certificate identifies at least a customer or the vehicle of the customer. With the OEM Prov certificate and its underlaying PCID, the customer/vehicle can be identified within the certificate infrastructure.

d) The Contract certificate is created and signed by the MO. The MO needs the PCID for this creation because the private key of the contract certificate will be encrypted by the OEM Prov certificate.

e) The Leaf Prov certificate is created to identify the trustworthy provisioning service. With this Leaf Prov certificate the provisioning service signs the MO's contract certificate chain so that the EVSE can verify the authenticity and integrity.

SEQ IDENTIFICATION, AUTHENTIFICATION AND AUTHORIZATION

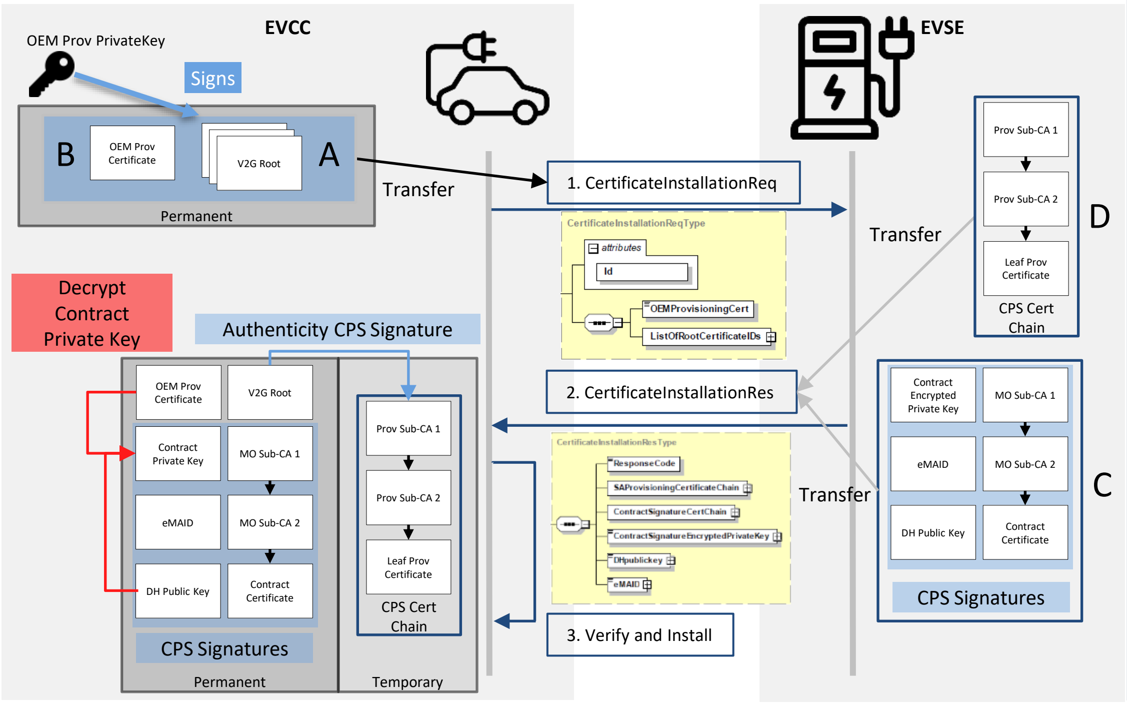
CertificateInstallationReq/Res



CONFIDENTIAL

SEQ IDENTIFICATION, AUTHENTIFICATION AND AUTHORIZATION

Certificate Installation



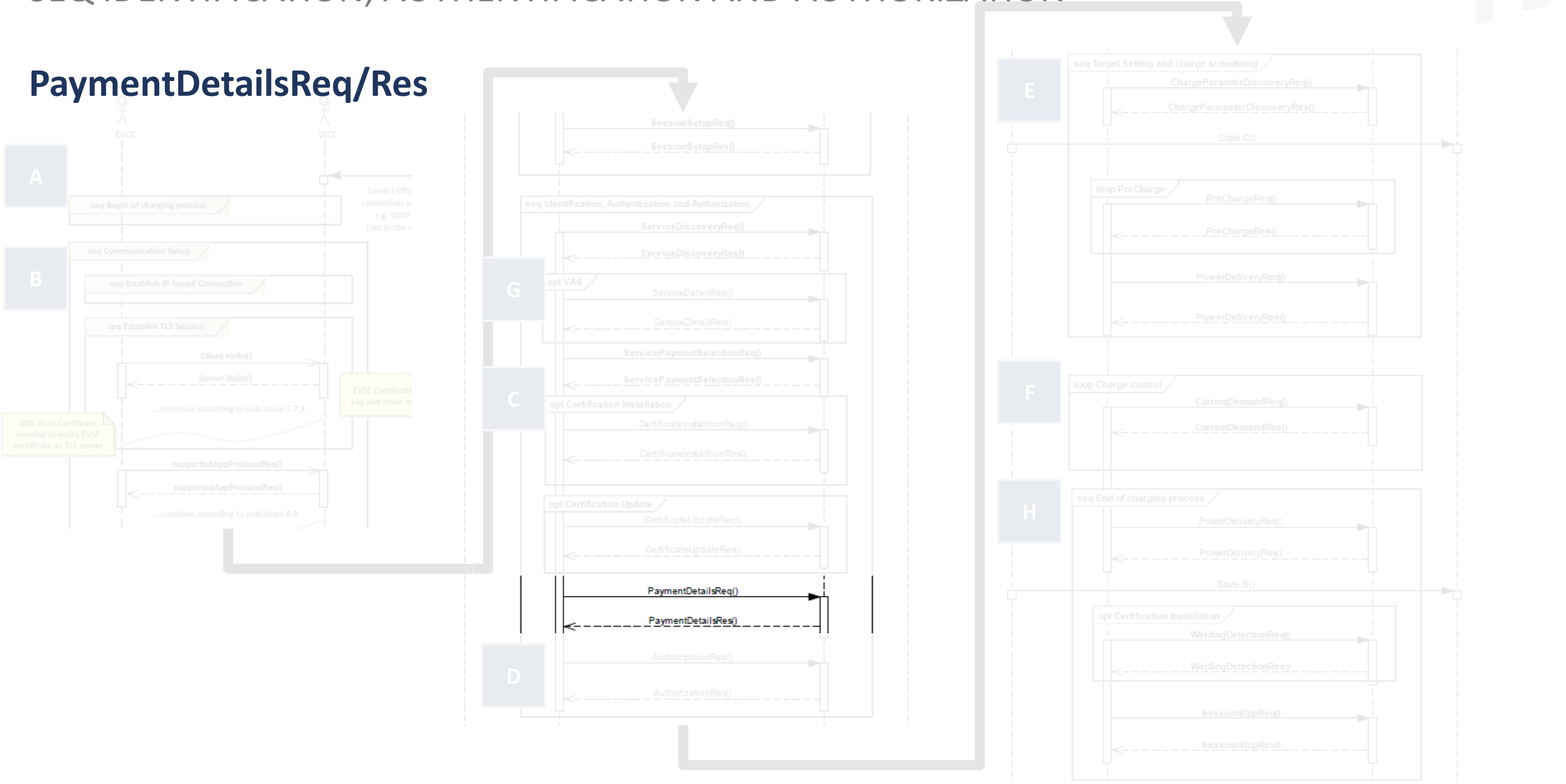
1. The vehicle sends the V2G Root Certificates (A) and the OEM Prov Certificate Public Key with the message CertificateInstallationReq and signs that message with the OEM Prov Certificate Private Key (B), so the CPS can verify authenticity of the request. The request is rooted through the EVSE-CPO infrastructure.
2. The EVSE sends the Contract Certificate Chain, eMAID, the encrypted Contract Certificate Private Key and the DH Public Key (C) that all have been signed by the Contract Provisioning Service Certificate Chain (D) within the CertificateInstallationRes response.
3. The EVCC can verify the authenticity of the transferred contract certificate chain by the signatures of the CPS with the Leaf Prov certificate chain. With the CPS DH public key and the OEM Prov certificate private key, the EVCC can decrypt the Contract certificate private key.

ECDH:

- DHPublicKey: 65Byte
- Contract Encrypted Private Key: 48Byte (16Byte initialization vector + 32Byte encrypted private key)

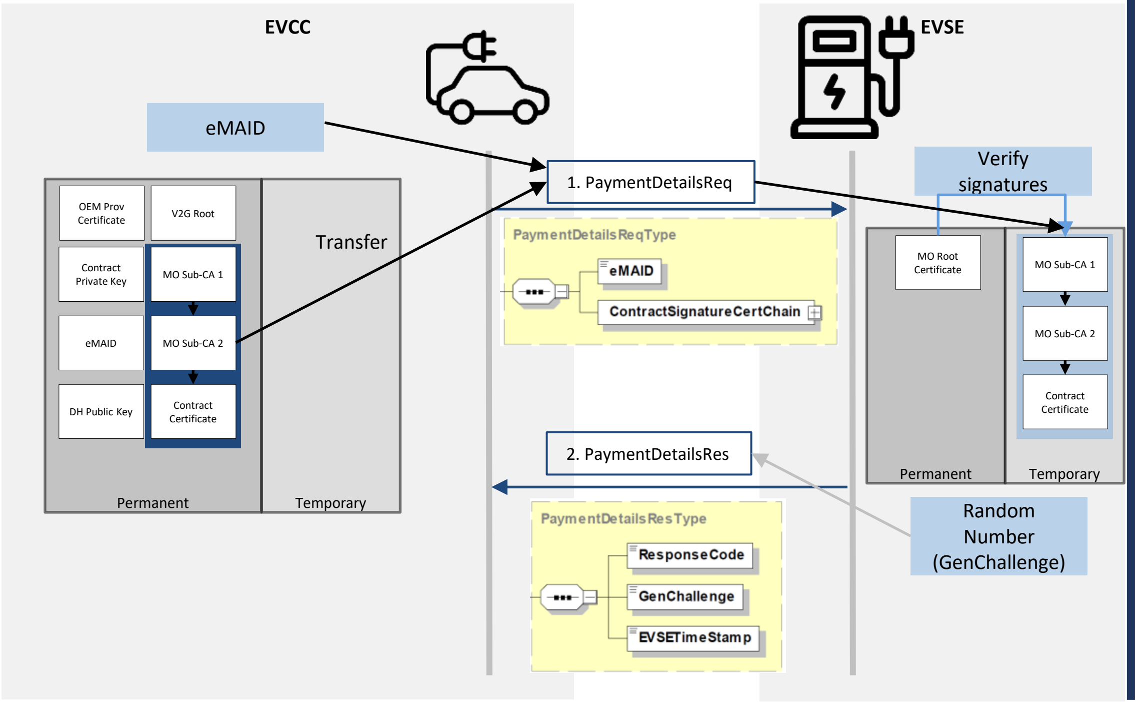
SEQ IDENTIFICATION, AUTHENTIFICATION AND AUTHORIZATION

PaymentDetailsReq/Res


EVCC
SECC
A
seq Begin of charging process
B
seq Communication Setup
seq Establish IP-based Connection
seq Establish TLS Session
Client Hello()
Server Hello()
... continue according to subclause 7.7.3
V2G Root Certificate needed to verify EVSE certificate as TLS server
supportedAppProtocolReq()
supportedAppProtocolRes()
... continue according to subclause 8.8
SessionSetupReq()
SessionSetupRes()
seq Identification, Authentication and Authorization
ServiceDiscoveryReq()
ServiceDiscoveryRes()
G
opt VAS
ServiceDetailReq()
ServiceDetailRes()
ServicePaymentSelectionReq()
ServicePaymentSelectionRes()
C
opt Certification Installation
CertificateInstalltionReq()
CertificateInstalltionRes()
opt Certification Update
CertificateUpdateReq()
CertificateUpdateRes()
PaymentDetailsReq()
PaymentDetailsRes()
D
AuthorizationReq()
AuthorizationRes()
E
seq Target Setting and charge scheduling
ChargeParamterDiscoveryReq()
ChargeParameterDiscoveryRes()
State C()
loop PreCharge
PreChargeReq()
PreChargeRes()
PowerDeliveryReq()
PowerDeliveryRes()
F
loop Charge control
CurrentDemandReq()
CurrentDemandRes()
H
seq End of charging process
PowerDeliveryReq()
PowerDeliveryRes()
State B()
opt Certification Installation
WeldingDetectionReq()
WeldingDetectionRes()
SessionStopReq()
SessionStopRes()

SEQ IDENTIFICATION, AUTHENTIFICATION AND AUTHORIZATION

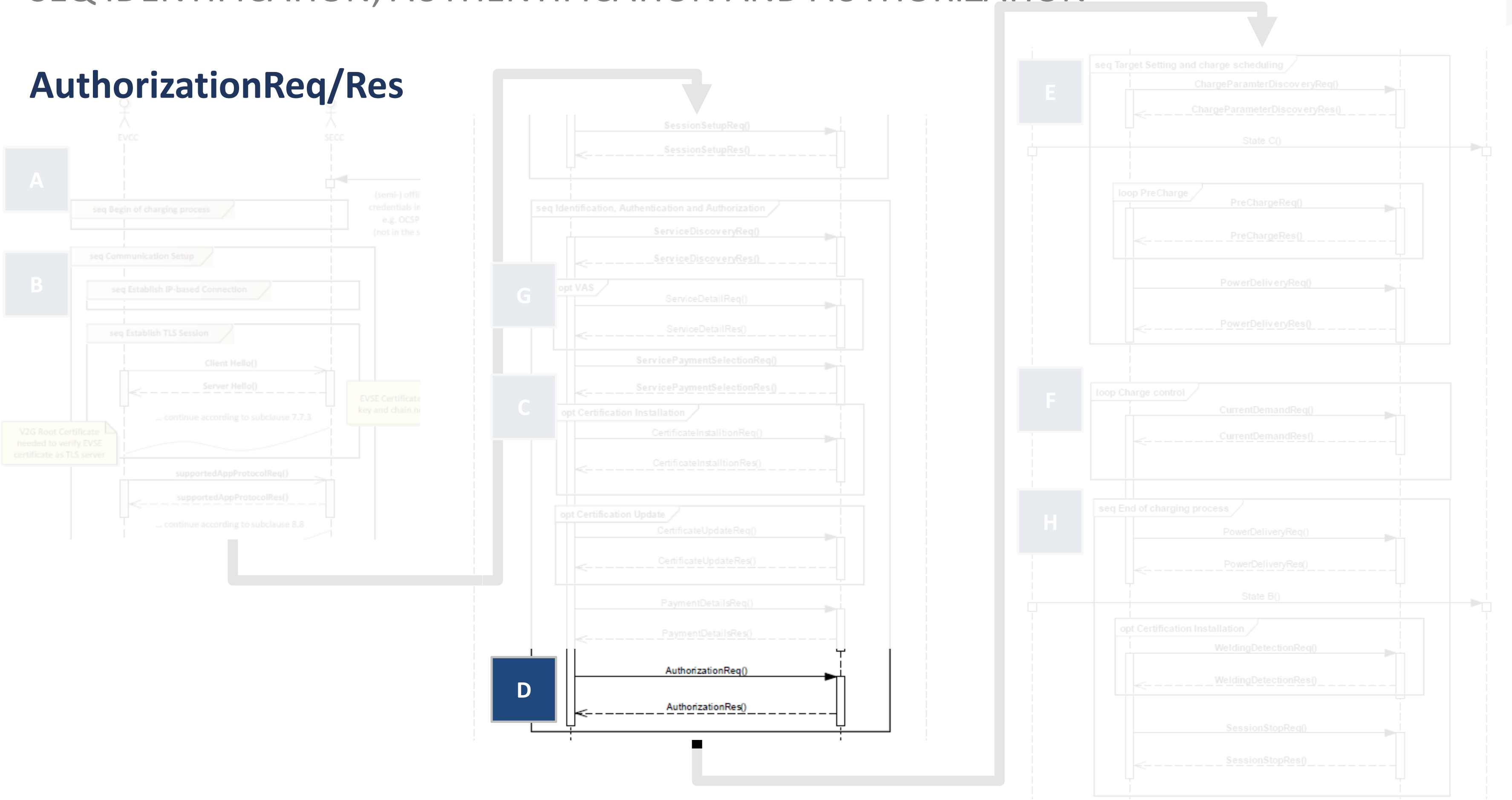
PaymentDetailsReq/Res



1. The EVCC sends the Contract Certificate Chain and eMAID within the PaymentDetailsReq request to the EVSE.
2. The EVSE verifies the EVCC's authenticity with the Contract Certificate Chain and the stored MO Root Certificate.
3. After the verification the EVSE sends the result and a random number to the EVCC within the PaymentDetailsRes response.

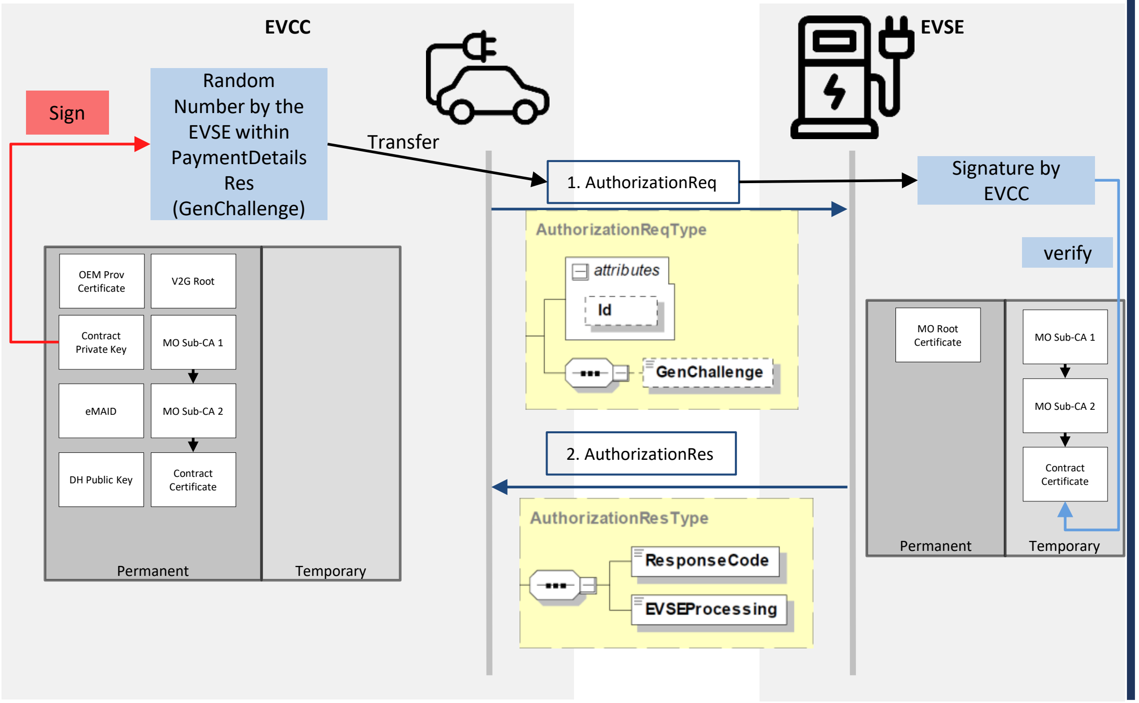
SEQ IDENTIFICATION, AUTHENTIFICATION AND AUTHORIZATION

AuthorizationReq/Res



EVCC
SECC
A
seq Begin of charging process
(semi-) offli credentials in e.g. OCSP (not in the s
B
seq Communication Setup
seq Establish IP-based Connection
seq Establish TLS Session
Client Hello()
Server Hello()
EVSE Certificate key and chain n
... continue according to subclause 7.7.3
V2G Root Certificate needed to verify EVSE certificate as TLS server
supportedAppProtocolReq()
supportedAppProtocolRes()
... continue according to subclause 8.8
SessionSetupReq()
SessionSetupRes()
seq Identification, Authentication and Authorization
ServiceDiscoveryReq()
ServiceDiscoveryRes()
G
opt VAS
ServiceDetailReq()
ServiceDetailRes()
ServicePaymentSelectionReq()
ServicePaymentSelectionRes()
C
opt Certification Installation
CertificateInstalltionReq()
CertificateInstalltionRes()
opt Certification Update
CertificateUpdateReq()
CertificateUpdateRes()
PaymentDetailsReq()
PaymentDetailsRes()
D
AuthorizationReq()
AuthorizationRes()
E
seq Target Setting and charge scheduling
ChargeParamterDiscoveryReq()
ChargeParameterDiscoveryRes()
State C()
loop PreCharge
PreChargeReq()
PreChargeRes()
PowerDeliveryReq()
PowerDeliveryRes()
F
loop Charge control
CurrentDemandReq()
CurrentDemandRes()
H
seq End of charging process
PowerDeliveryReq()
PowerDeliveryRes()
State B()
opt Certification Installation
WeldingDetectionReq()
WeldingDetectionRes()
SessionStopReq()
SessionStopRes()

AuthorizationReq/Res



1. The EVCC sends back the GenChallenge received previous by the EVSE within the AuthorizationReq request to the EVSE. Additionally the message gets signed by the contract private key to make sure, it is definitely the right and authentic EVCC the EVSE is talking to.
2. The EVSE verifies the EVCC's authenticity through the signature with the contract certificate chain previously received by the EVCC within the PaymentDetailsReq request and checks the GenChallenge is the same as the EVSE send to the EVCC within the PaymentDetailsRes response.
3. After the verification the EVSE sends the result to the EVCC.

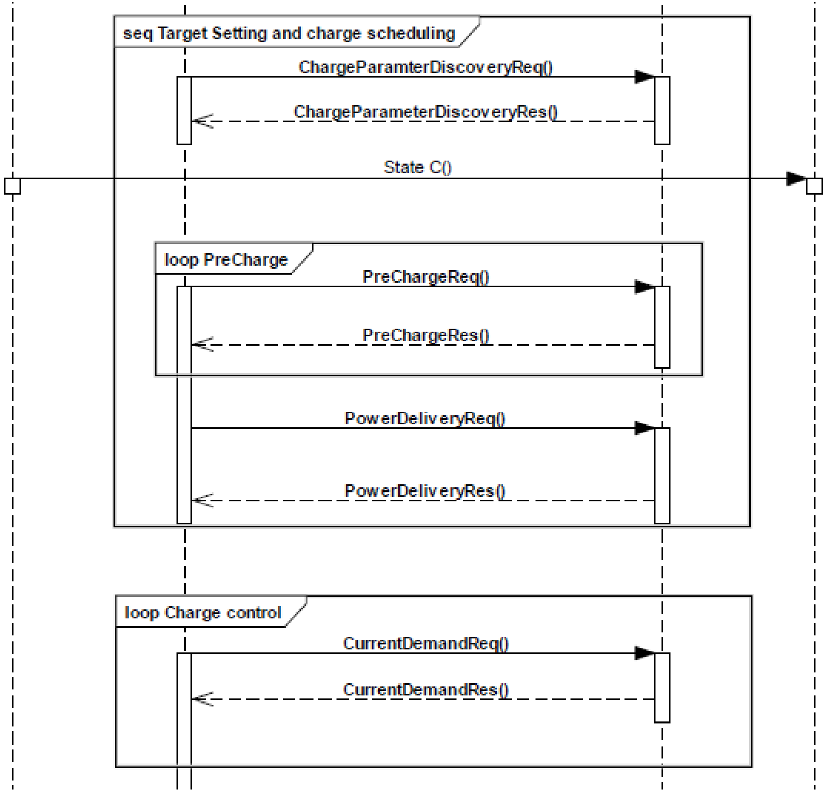
Agenda

1 Some Basics regarding ISO 15118

2 ISO 15118 Structure

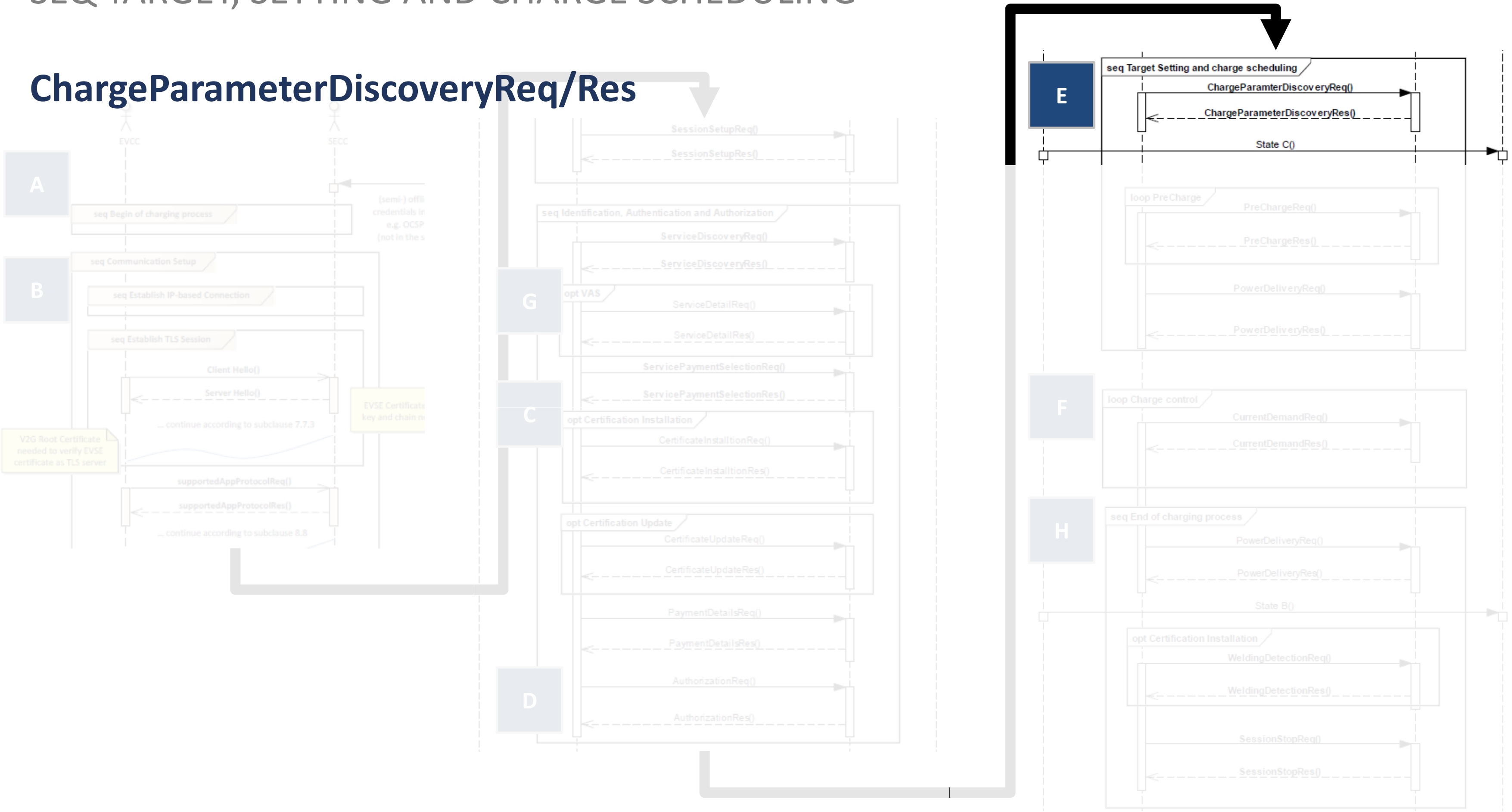
- 2.1 Begin of Charging
- 2.2 TLS Session Setup
- 2.3 Session Setup and Services
- 2.4 Certificate Handling
- 2.5 **Charging Procedure**

3 Not described within ISO 15118 but required



SEQ TARGET, SETTING AND CHARGE SCHEDULING

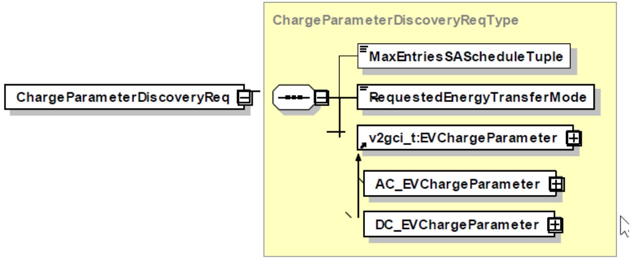
ChargeParameterDiscoveryReq/Res

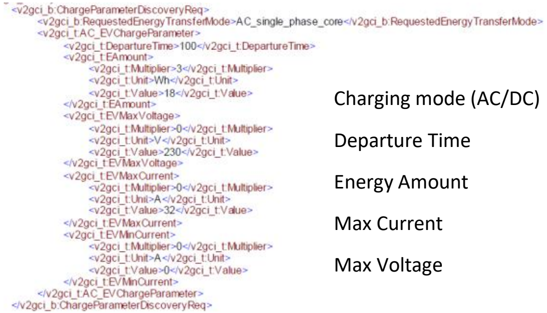

E
seq Target Setting and charge scheduling
ChargeParamterDiscoveryReq()
ChargeParameterDiscoveryRes()
State C()
A
B
C
D
F
G
H
EVCC
SECC
seq Begin of charging process
seq Communication Setup
seq Establish IP-based Connection
seq Establish TLS Session
Client Hello()
Server Hello()
... continue according to subclause 7.7.3
supportedAppProtocolReq()
supportedAppProtocolRes()
... continue according to subclause 8.8
V2G Root Certificate needed to verify EVSE certificate as TLS server
SessionSetupReq()
SessionSetupRes()
seq Identification, Authentication and Authorization
ServiceDiscoveryReq()
ServiceDiscoveryRes()
opt VAS
ServiceDetailReq()
ServiceDetailRes()
ServicePaymentSelectionReq()
ServicePaymentSelectionRes()
opt Certification Installation
CertificateInstalltionReq()
CertificateInstalltionRes()
opt Certification Update
CertificateUpdateReq()
CertificateUpdateRes()
PaymentDetailsReq()
PaymentDetailsRes()
AuthorizationReq()
AuthorizationRes()
loop PreCharge
PreChargeReq()
PreChargeRes()
PowerDeliveryReq()
PowerDeliveryRes()
loop Charge control
CurrentDemandReq()
CurrentDemandRes()
seq End of charging process
PowerDeliveryReq()
PowerDeliveryRes()
State B()
opt Certification Installation
WeldingDetectionReq()
WeldingDetectionRes()
SessionStopReq()
SessionStopRes()

SEQ TARGET, SETTING AND CHARGE SCHEDULING

ChargeParameterDiscoveryReq

Schema of ChargeParameterDiscoveryReq


ChargeParameterDiscoveryReqType
ChargeParameterDiscoveryReq
MaxEntriesSAScheduleTuple
RequestedEnergyTransferMode
v2gci_t:EVChargeParameter
AC_EVChargeParameter
DC_EVChargeParameter



```
<v2gci_b:ChargeParameterDiscoveryReq>
    <v2gci_b:RequestedEnergyTransferMode>AC_single_phase_core</v2gci_b:RequestedEnergyTransferMode>
    <v2gci_t:AC_EVChargeParameter>
        <v2gci_t:DepartureTime>100</v2gci_t:DepartureTime>
        <v2gci_t:EAmount>
            <v2gci_t:Multiplier>3</v2gci_t:Multiplier>
            <v2gci_t:Unit>Wh</v2gci_t:Unit>
            <v2gci_t:Value>18</v2gci_t:Value>
        </v2gci_t:EAmount>
        <v2gci_t:EVMaxVoltage>
            <v2gci_t:Multiplier>0</v2gci_t:Multiplier>
            <v2gci_t:Unit>V</v2gci_t:Unit>
            <v2gci_t:Value>230</v2gci_t:Value>
        </v2gci_t:EVMaxVoltage>
        <v2gci_t:EVMaxCurrent>
            <v2gci_t:Multiplier>0</v2gci_t:Multiplier>
            <v2gci_t:Unii>A</v2gci_t:Unit>
            <v2gci_t:Value>32</v2gci_t:Value>
        </v2gci_t:EVMaxCurrent>
        <v2gci_t:EVMinCurrent>
            <v2gci_t:Multiplier>0</v2gci_t:Multiplier>
            <v2gci_t:Unit>A</v2gci_t:Unit>
            <v2gci_t:Value>0</v2gci_t:Value>
        </v2gci_t:EVMinCurrent>
    </v2gci_t:AC_EVChargeParameter>
</v2gci_b:ChargeParameterDiscoveryReq>
```

Charging mode (AC/DC)

Departure Time

Energy Amount

Max Current

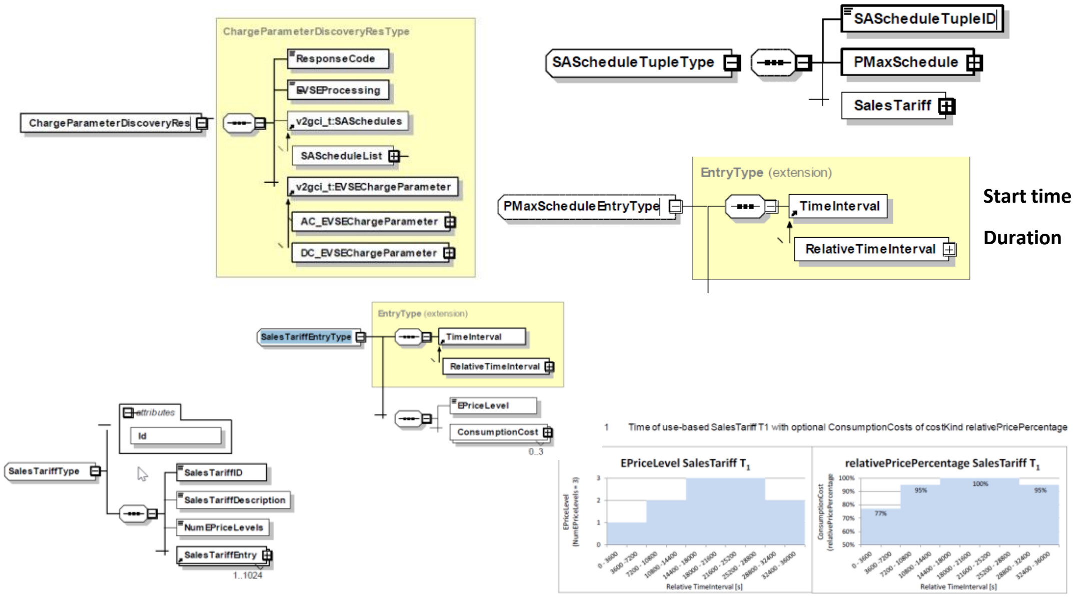
Max Voltage

Description

- **After being authorized for charging at the EVSE (SECC) the EVCC and the SECC negotiate the charging**
- ***"…ensure that the client (e.g. EV) will be satisfied…"***
- **Initially, before the onset of the energy supply, the EV will negotiate with EVSE operator, and third party actors indirectly, to fit to the known or predicted available electric power.**

ChargeParameterDiscoveryRes

Schema of ChargeParameterDiscoveryRes



Start time

Duration

1 Time of use-based SalesTariff T1 with optional ConsumptionCosts of costKind relativePricePercentage

Description

- **According to the requested ChargingParameterDiscoveryReq, the EVSE provides charging plans.**
- **Charging plan relevant parameters are provided within**
  - **SAScheduleTupleType, which inclused PMaxSchedule including required power, start time and duration**
  - **SalesTariff, providing time intervals with corresponding price levels**

Agenda

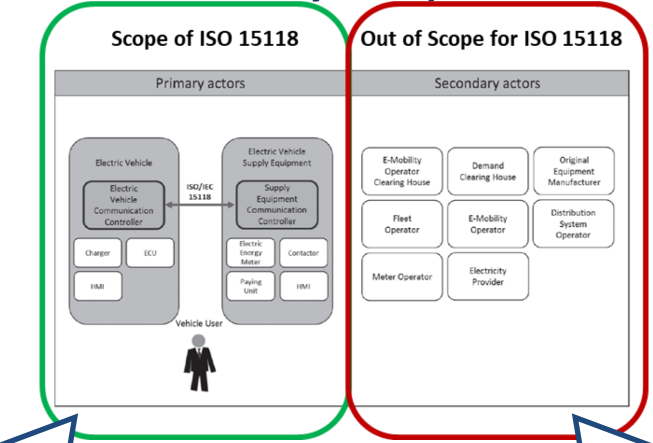
1 Some Basics regarding ISO 15118

2 ISO 15118 Structure

3 Not described within ISO 15118 but required

SCOPE OF ISO 15118

ISO 15118 defines a clear line between scope (EV-EVSE communication) and out of scope content (secondary actors, interaction, ecosystem).

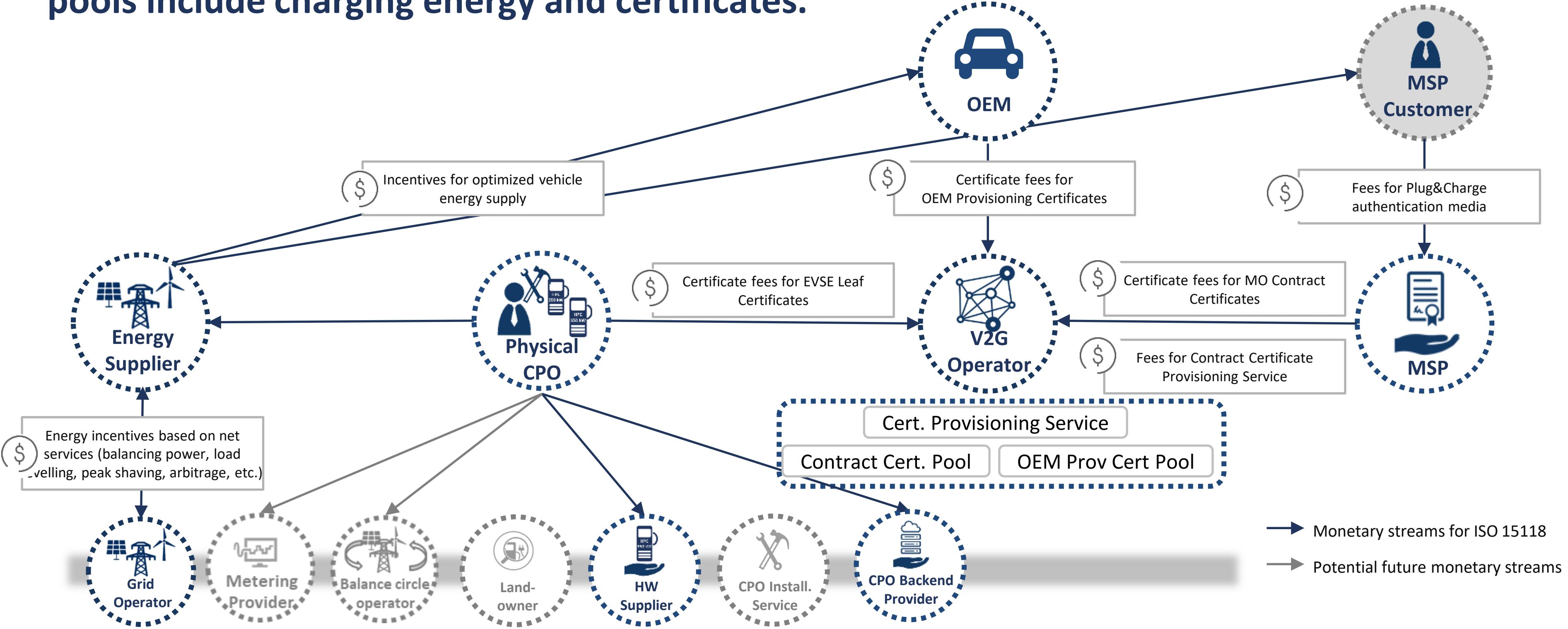

Scope of ISO 15118
Out of Scope for ISO 15118
Primary actors
Secondary actors
Electric Vehicle
Electric Vehicle Communication Controller
Charger
ECU
HMI
ISO/IEC 15118
Electric Vehicle Supply Equipment
Supply Equipment Communication Controller
Electric Energy Meter
Contactor
Paying Unit
HMI
Vehicle User
E-Mobility Operator Clearing House
Demand Clearing House
Original Equipment Manufacturer
Fleet Operator
E-Mobility Operator
Distribution System Operator
Meter Operator
Electricity Provider

- Standardized EV - EVSE communication
- Little to no space regarding utilizing blockchain as technology
- Potential blockchain approaches must follow an „ISO 15118 simulator“ like approach

- Potentials for blockchain forging an ISO 15118 ecosystem
- Roles of MO and V2G Operator most proising
- MO functions can be fully adopted to private charging (PE)

MONETARY STREAMS OF ISO 15118 WITHIN THE ECOSYSTEM.

ISO 15118 creates new revenue streams within the charging ecosystem. The biggest value pools include charging energy and certificates.


OEM
MSP Customer
$ Incentives for optimized vehicle energy supply
$ Certificate fees for OEM Provisioning Certificates
$ Fees for Plug&Charge authentication media
Energy Supplier
Physical CPO
$ Certificate fees for EVSE Leaf Certificates
V2G Operator
$ Certificate fees for MO Contract Certificates
$ Fees for Contract Certificate Provisioning Service
MSP
Cert. Provisioning Service
Contract Cert. Pool
OEM Prov Cert Pool
$ Energy incentives based on net services (balancing power, load levelling, peak shaving, arbitrage, etc.)
Grid Operator
Metering Provider
Balance circle operator
Land-owner
HW Supplier
CPO Install. Service
CPO Backend Provider
Monetary streams for ISO 15118
Potential future monetary streams

Backup: New Agenda