

DIN EN ISO 15118-20/A1**DIN**

ICS 43.120

Einsprüche bis 2025-03-17
 Vorgesehen als Änderung von
 DIN EN ISO 15118-20:2022-12

Entwurf

**Straßenfahrzeuge –
 Kommunikationsschnittstelle zwischen Fahrzeug und Ladestation –
 Teil 20: Anforderungen der 2. Generation an das Netzwerk- und
 Anwendungsprotokoll – ÄNDERUNG 1: AC DER-Dienst, MCS-Dienst und
 verbessertes Security Konzept (ISO 15118-20:2022/DAM 1:2024);
 Englische Fassung EN ISO 15118-20:2022/prA1:2024**

Road vehicles –

Vehicle to grid communication interface –

Part 20: 2nd generation network layer and application layer requirements –

AMENDMENT 1: AC DER service, MCS service, and improved security concept
 (ISO 15118-20:2022/DAM 1:2024);

English version EN ISO 15118-20:2022/prA1:2024

Véhicules routiers –

Interface de communication entre véhicule et réseau électrique –

Partie 20: Exigences des couches réseau et application de 2ème génération –

AMENDEMENT 1: Service AC DER, service MCS et concept de sécurité amélioré
 (ISO 15118-20:2022/DAM 1:2024);

Version anglaise EN ISO 15118-20:2022/prA1:2024

Anwendungswarnvermerk

Dieser Entwurf mit Erscheinungsdatum 2025-01-17 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil das beabsichtigte Dokument von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an naautomobil@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Auto und Mobilität (NAAutomobil), 10004 Berlin, Postfach 8 04 62 oder Behrenstr. 35, 10117 Berlin.

Es wird gebeten, mit den Kommentaren zu diesem Entwurf jegliche relevanten Patentrechte, die bekannt sind, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 184 Seiten

DIN-Normenausschuss Auto und Mobilität (NAAutomobil)



E DIN EN ISO 15118-20/A1:2025-02**Nationales Vorwort**

Das Dokument EN ISO 15118-20:2020/prA1:2024 wurde vom Technischen Komitee ISO/TC 22 „Road vehicles“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 301 „Straßenfahrzeuge“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Normungsgremium ist der Arbeitsausschuss NA 052-00-31 AA „Datenkommunikation“ im DIN-Normenausschuss Auto und Mobilität (NAAutomobil).

Dieses Dokument enthält unter Berücksichtigung des DIN-Präsidialbeschlusses 1/2004 nur die Englische Fassung von EN ISO 15118-20:2020/prA1:2024.

Der Bedarf für eine Deutsche Fassung wird derzeit beraten.

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 15118-10:202X siehe DIN EN ISO 15118-10

Um den Energieverbrauch von Fahrzeugen zu senken, werden Fahrzeuge mit elektrischem Teil- oder Komplettantrieb entwickelt. Um die Batterien dieser Fahrzeuge aufladen zu können, wird eine spezielle Lade-Infrastruktur benötigt.

Während verschiedene Teilaufgaben in der Normung von Elektrofahrzeugen und Infrastruktur bei ISO und IEC bereits behandelt wurden, beschäftigt sich diese Normenreihe mit dem Informationsaustausch zwischen Elektrofahrzeug und Lade-Infrastruktur. Kommunikation ist für das effektive Aufladen von Fahrzeugen sowie die Entwicklung effizienter und komfortabler Abrechnungssysteme unabdingbar.

Dieser Teil der Normenreihe legt Anforderungen an die Übertragung von Botschaften mittels Zweidraht Ethernet fest.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA

(informativ)

Begriffe

Es wurden die folgenden Begriffe am Ende des Abschnittes ergänzt.

3.72

Lade Freigabezustand

CE state, en: charge enable state

Zustand nach der Ladefreigabefunktion, die in IEC 61851-23-3 festgelegt ist

3.73

Megawatt Ladesystem

MCS, en: megawatt charging system

Ladesystem nach IEC 61851-23-3

3.74

Ende der Energieerzeugung

en **cease to energize**

Beendigung der aktiven Leistungsversorgung unter stationären und vorübergehenden Bedingungen und Grenzungen rückwirkendem Leistungsaustausches

Anmerkung 1 zum Begriff: Nachdem die Beendigung vorbei ist, darf das Elektrofahrzeug direkt wieder in Betrieb genommen werden, ohne dabei die Serviceregeln für den Eintritt zu berücksichtigen.

3.75

verteilte Energiequelle

DER, en: distributed energy resource

elektrische Energiequelle, die nicht direkt mit einem Übertragungssystem verbunden ist

BEISPIEL Generatoren und Energiespeichersysteme die in der Lage sind, Energie in ein elektrisches Netz einzubringen.

Anmerkung 1 zum Begriff: Ein Kopplungssystem oder ein unterstützendes DER-System das in Übereinstimmung mit diesem Dokument als Teil einer DER notwendig ist.

3.76

Diensteingabe

en **enter service**

Menge von Parametern die festlegen, wie im elektrischen Energiesystem die Stromversorgung gestartet und beendet werden kann

Anmerkung 1 zum Begriff: Wenn die Spannungs- und die Frequenzwerte nicht im gewünschten Bereich sind, wird der DER die Einspeisung von Energie an das Netz/elektrische Energiesystem nicht erlaubt werden.

3.77

Frequenz-Regeldifferenzkurve

en **frequency droop curve**

parametrisierbare Kurve der Frequenz-Watt-Funktion

Anmerkung 1 zum Begriff: Diese Parameter beinhalten eine Frequenz dB (tote Zone) und ein einheitsloser Faktor k, der die Rate der Leistungsausgangsänderung bezogen auf die Frequenzänderung festlegt. Diese Betriebsgrenzen die aktive Leistungserzeugung oder den Verbrauch, wenn die Netzfrequenz vom Normalwert von einen festgelegten Wert abweicht.

E DIN EN ISO 15118-20/A1:2025-02**3.78****Stufe-1 Laden****en level 1 charging**

Laden mit einer maximalen Leistung zwischen 1 kW und 1,8 kW über eine übliche einphasige 120 Vrms Wechselspannungsdoce

Anmerkung 1 zum Begriff: Diese Leistungsbegrenzung gilt nur in den USA.

3.79**Stufe-2 Laden****en level 2 charging**

Laden mit einer maximalen Leistung zwischen 3 kW und 22 kW über den zugehörigen Wechselspannungslader

Anmerkung 1 zum Begriff: In den USA liegt die typische Versorgungsspannung bei 240 Vrms, wohingegen diese in Europa bei 230 Vrms liegt.

3.80**möglicher Auslösebereich****en may trip region**

Spannungs- oder Frequenzbereich, indem dem Elektrofahrzeug erlaubt ist, die Energieerzeugung zu beenden und die Verbindung auszulösen

Anmerkung 1 zum Begriff: Der Bereich ist durch eine stückweise lineare Kurve festgelegt, welche die Spannungs- oder Frequenzgrenzen markiert.

3.81**momentaner Beendigungsbereich****en momentary cessation region**

Spannungs- oder Frequenzbereich, indem das Elektrofahrzeug die Energieerzeugung (Energieeinspeisung) für ein elektrisches Energiesystem temporär beendet, als Reaktion auf eine Störung der verfügbaren Spannungen oder der Systemfrequenz

Anmerkung 1 zum Begriff: Wenn dieser Bereich erreicht wird, erhält das EV die Fähigkeit der unverzüglichen Wiederherstellung des Betriebszustandes zurück, sobald die verfügbaren Spannungen und die Systemfrequenz wieder innerhalb der festgelegten Grenzen liegen.

Anmerkung 2 zum Begriff: Das Gebiet ist durch eine stückweise lineare Kurve festgelegt, welche die Spannungs- oder Frequenzgrenzen markiert.

3.82**Muss-Auslösebereich****en must trip region**

Spannungs- oder Frequenzbereich, indem das Elektrofahrzeug die Energieerzeugung beenden muss und die Verbindung auslöst

Anmerkung 1 zum Begriff: Der Bereich ist durch eine stückweise lineare Kurve festgelegt, welche die Spannungs- oder Frequenzgrenzen markiert.

3.83**Antwortzeit des offenen Regelkreises****en open loop response time**

Zeit, die benötigt wird, 90 % der Sprungantwort des Regeleingangssignals zu erreichen

3.84**übersteuerter Ansteuerungstyp**en **over-excited excitation type**

Ansteuerungstyp, bei dem die DER dem/das System (mit) Blindleistung einspeist/versorgt

Anmerkung 1 zum Begriff: Eine übersteuerte DER speist/versorgt ein System mit Blindleistung. Der Begriff wird im Allgemeinen mit Synchronmaschinen (Motoren oder Generatoren) in Verbindung gebracht. Im Generatorbetrieb folgt in einem übersteuerten DER der Strom der Spannung (Blindleistung > 0) und die Blindleistungseinspeisung neigt zur Erhöhung der Systemspannung.

3.85**Diensterlaubnis**en **permit service**

Einstellung die anzeigen, ob einer DER erlaubt ist, in Dienst zu treten oder zu bleiben

3.86**Dienstrückkehr**en **return to service**

Diensteintritt, nach einer Erholung von einer Auslösung

3.87**Durchtritt**en **ride trough**

Fähigkeit, Spannungs- oder Frequenzstörungen innerhalb festgelegter Grenzen standzuhalten, und den Betrieb, wie festgelegt, fortzuführen

3.88**Auslösung**en **trip**

Sperrung der unmittelbaren Rückkehr in den Betriebsmodus

Anmerkung 1 zum Begriff: Wenn die DER die Erlaubnis erhält, den Betriebsmodus fortzusetzen, muss diese den Eintrittsregeln folgen.

3.89**untersteuerter Ansteuerungstyp**en **under-excited excitation type**

Ansteuerungstyp, bei dem die DER Blindleistung vom System absorbiert/verbraucht

Anmerkung 1 zum Begriff: Eine untersteuerte DER absorbiert/verbraucht vom System Blindleistung. Der Begriff wird im Allgemeinen mit Synchronmaschinen (Motoren oder Generatoren) in Verbindung gebracht. Im Generatorbetrieb in einem übersteuerten DER folgt die Spannung dem Strom (Blindleistung < 0) und die Blindleistungsabsorption neigt zur Absenkung der Systemspannung.

E DIN EN ISO 15118-20/A1:2025-02

Nationaler Anhang NB
(informativ)

Literaturhinweise

DIN EN ISO 15118-10, Straßenfahrzeuge — Kommunikationsschnittstelle zwischen Fahrzeug und Ladestation — Teil 10: Anforderungen an die physikalische Schicht und Sicherungsschicht für Zweidraht Ethernet

- Entwurf -
E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 31, *Data communication*.

A list of all parts in the ISO 15118 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Road vehicles — Vehicle to grid communication interface —

Part 20: 2nd generation network layer and application layer requirements

AMENDMENT 1: AC DER service, MCS service, and improved security concept

Clause 2

Add the following references at the end of this clause:

ISO 15118-10:202X, *Road vehicles – Vehicle-to-grid communication interface – Part 10: Physical layer and data link layer requirements for single-pair Ethernet*.

IEC 61851-23-3:202X, *Electrical power/energy transfer systems for electrically propelled road vehicles and industrial trucks*.

Clause 3

Add the following terms and definitions at the end of this clause:

3.72

charge enable state
CE state

state according to the charge enable function defined in IEC 61851-23-3

3.73

megawatt charging system
MCS

charging system according to IEC 61851-23-3

3.74

cease to energize

cessation of active power delivery under steady-state and transient conditions and limitation of reactive power exchange

Note 1 to entry: After the cessation is over, the EV is allowed to return immediately into service without following the enter service rules.

3.75

distributed energy resource
DER

source of electric power that is not directly connected to a bulk power system.

EXAMPLE Generators and energy storage technologies capable of exporting active power to the electrical grid.

Note 1 to entry: An interconnection system or a supplemental DER device that is necessary for compliance with this document is part of a DER.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

3.76**enter service**

set of parameters that defines how to start energizing or re-energizing the electric power system

Note 1 to entry: If voltage and frequency values are not within the desired range, the DER will not be allowed to start injecting power to the grid/electric power system.

3.77**frequency droop curve**

parameterized curve of the frequency-watt function

Note 1 to entry: The parameters include a frequency dB (dead band) and a unitless factor k which defines the rate of power output change due to the frequency change. This operation limits active power generation or consumption when the line frequency deviates from nominal by a specified amount.

3.78**level 1 charging**

charging with a maximum power between 1 kW and 1,8 kW, via a standard 120 Vrms AC single phase outlet

Note 1 to entry: This power limit is only applicable in the US.

3.79**level 2 charging**

charging with a maximum power between 3 kW and 22 kW, via a dedicated AC charger

Note 1 to entry: In the US the voltage supplied is typically 240 Vrms AC whereas in Europe is 230 Vrms AC.

3.80**may trip region**

region of voltage or frequency within which the EV is allowed to cease to energize and to trip the connection

Note 1 to entry: The region is defined by a piecewise linear curve demarcating the boundary for voltage or frequency.

3.81**momentary cessation region**

region of voltage or frequency within which the EV will temporarily cease to energize (inject power to) an electric power system in response to a disturbance of the applicable voltages or the system frequency

Note 1 to entry: When entering this region, the EV will retain the capability of immediate restoration of the output of operation when the applicable voltages and the system frequency return to within the defined ranges.

Note 2 to entry: The region is defined by a piecewise linear curve demarcating the boundary for voltage or frequency.

3.82**must trip region**

region of voltage or frequency within which the EV must cease to energize and must trip the connection

Note 1 to entry: The region is defined by a piecewise linear curve demarcating the boundary for voltage or frequency.

3.83**open loop response time**

time to ramp up to 90 % of the new target in response to the step change of the control input signal

3.84**over-excited excitation type**

excitation type, where a DER injects/supplies reactive power to the system

Note 1 to entry: An over-excited DER injects/supplies reactive power to the system. The term is usually associated with synchronous machines (motors or generators). In generator sign convention, an over-excited DER has its current lagging the voltage (reactive power > 0) and the reactive power injection tends to increase the system voltage.

3.85**permit service**

setting that indicates whether a DER is allowed to enter or remain in service

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

3.86

return to service

enter service following recovery from a trip

3.87

ride-through

ability to withstand voltage or frequency disturbances inside defined limits and to continue operating as specified

3.88

trip

inhibition of immediate return to service

Note 1 to entry: Once the DER has permission to come back to service, it must follow the enter service rules.

3.89

under-excited excitation type

excitation type, where a DER absorbs/consumes reactive power from the system

Note 1 to entry: An under-excited DER absorbs/consumes reactive power from the system. The term is usually associated with synchronous machines (motors or generators). In generator sign convention, an under-excited DER has its current leading the voltage (reactive power < 0) and the reactive power absorption tends to decrease the system voltage.

Clause 6

Replace Figure 2 with this figure:

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

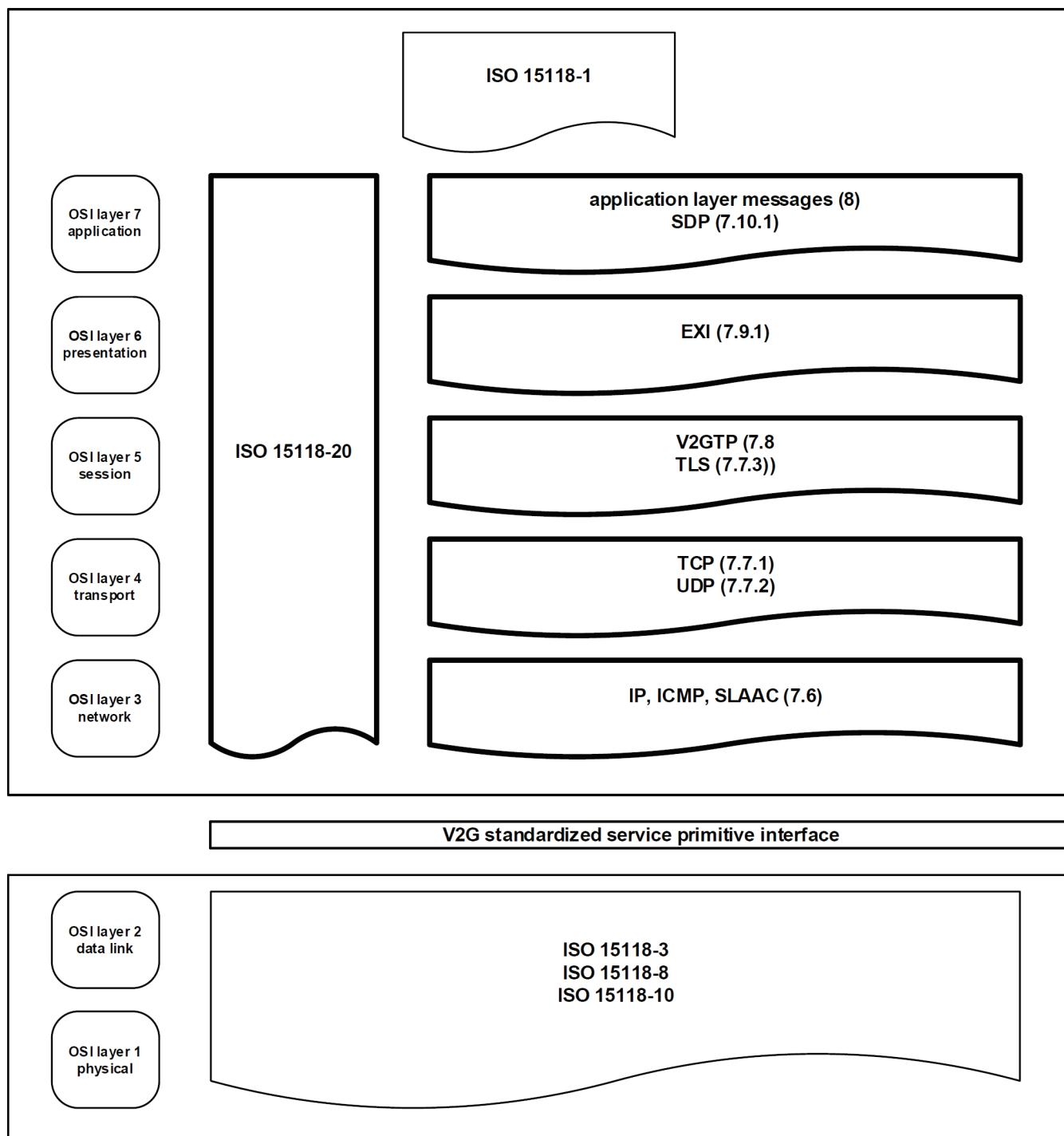


Figure 2 — Vehicle to grid communication document overview

Clause 7.3.2

Replace Table 2 with this table:

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table 2 — Certificate extension examples

Certificate extensions	Description
Key usage	Usage of the corresponding private key (e.g. Digital Signature, non-repudiation, key encipherment, ...)
Extended Key Usage	<p>Further specification of key usage using OIDs, e.g.:</p> <ul style="list-style-type: none"> — server authentication (1.3.6.1.5.5.7.3.1) — client authentication (1.3.6.1.5.5.7.3.2) <p>NOTE Sometimes the following values are encoded here:</p> <ul style="list-style-type: none"> — Netscape SGC (1.3.6.1.4.1.311.10.3.3) — Microsoft SGC (2.16.840.1.113730.4.1) <p>SGC stands for server gated crypto and indicates that the server can also use strong cryptography for the connection with the client's browser. This extension was used at the time of strong crypto export control to enable financial web site to provide appropriate protection of the data transfer.</p>
CRL distribution point	Location to retrieve certificate revocation lists
OCSP	Location to retrieve OCSP. Refer to IETF RFC 6960 as updated by IETF RFC 8954 for details.
Authority information	Additional authorization information
Subject alternative name	Alternative names of the entity
Basic constraint = CA	True if the certificate is a root certificate or a Sub-CA certificate.
Subject information	Additional information about the subject

Add the following new paragraph below NOTE 14 to requirement [V2G20-1234]:

In this document, the size of certificate is less than or equal to 1600 bytes. This limit considers resource constraints in embedded systems and complying secondary actors must be aware of this when they generate certificates. For example, it is recommended to be cautious when adding long URLs, 4-byte characters in distinguished names, or multiple certificate policies as these may increase the size of the certificate significantly. It can be necessary to use only one, either CRLDistributionPoints or AuthorityInfoAccess, and not both, if including both makes the certificate larger than 1600 bytes.

Replace requirement [V2G20-1004] with the following new requirements and NOTE:

[V2G20-3000] The relying parties shall ensure that the certificates are valid exclusively within the validity of their issuer's certificate.

NOTE 15 The CA is expected to only issue certificates that are valid exclusively within the validity of its own certificate.

[V2G20-3001] While validating certificates, EVCC and SECC shall ensure that **[V2G20-3000]** is fulfilled.

Replace first bullet point in NOTE 20 (old numbering) with:

NOTE 20 [...].

- The content of the leaf certificate has not been altered after issue. This means it is possible to check and confirm the signature up to the trust anchor level and thus the integrity of the signed content.
- [...].

Renumber old NOTE 15 and following notes, starting with number 16.

Clause 7.3.2.1

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Replace requirement [V2G20-2327] and NOTE 3 with:

- [V2G20-3002]** OCSP signer certificate used to sign the OCSP response for SECC certificate status shall be generated using a certificate chain that either uses the same V2G Root CA certificate as the trust anchor as the SECC certificate whose status is being checked or uses one of the V2G Root CA certificates, as the trust anchor, whose DN was included by the EVCC in the "certificateAuthorities" extension sent by the EVCC in the "ClientHello" message. Refer to Figure 5 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of certificate structure. Refer to Annex B for details of the certificate profile.

NOTE 3 This document does not mandate usage of a particular V2G Root CA. In case multiple V2G Root CAs are available in a region, a good practice would be that the OCSP signer certificate that signs the OCSP response for the SECC certificate (or the sub-CA certificate(s) in the SECC certificate chain) chains up to the same V2G Root CA that signs the SECC certificate chain that the SECC is transmitting to the EVCC for this particular TLS handshake. This is however out of scope of this document.

Replace requirements [V2G20-2330] and [V2G20-2332] with:

- [V2G20-3003]** OCSP signer certificate used to sign the OCSP response for contract certificate status shall be generated using a certificate chain that uses either the same eMSRP Root CA certificate or the same V2G Root CA certificate as the trust anchor as the contract certificate whose status is being checked. Refer to Figure 6 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of certificate structure. Refer to Annex B for details of the certificate profile.

- [V2G20-3004]** OCSP signer certificate used to sign the OCSP response for vehicle certificate status shall be generated using a certificate chain that uses either the same OEM Root CA certificate or the same V2G Root CA certificate as the trust anchor as the vehicle certificate whose status is being checked. Refer to Figure 7 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of certificate structure. Refer to Annex B for details of the certificate profile.

Replace NOTE 10 with:

NOTE 10 This document does not mandate usage of a particular V2G Root CA. In case multiple V2G Root CAs are available in a region, a good practice would be that the OCSP signer certificate that signs the OCSP response for the vehicle certificate (or the sub-CA certificate(s) in the vehicle certificate chain) chains up to the same V2G Root CA that signs the vehicle certificate chain whose status is being checked. This is however out of scope of this document.

Replace requirement [V2G20-2334] and NOTE 12 with:

- [V2G20-3005]** OCSP signer certificate used to sign the OCSP response for OEM provisioning certificate status shall be generated using a certificate chain that uses either the same OEM Root CA certificate or the same V2G Root CA certificate as the trust anchor as the OEM provisioning certificate whose status is being checked. Refer to Figure 7 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of certificate structure. Refer to Annex B for details of the certificate profile.

NOTE 12 This document does not mandate usage of a particular V2G Root CA. In case multiple V2G Root CAs are available in a region, a good practice would be that the OCSP signer certificate that signs the OCSP response for the OEM provisioning certificate (or the sub-CA certificate(s) in the OEM provisioning certificate chain) chains up to the same V2G Root CA that signs the OEM provisioning certificate chain whose status is being checked. This is however out of scope of this document.

Clause 7.3.4

Delete the following requirements: [V2G20-1235] and [V2G20-2646].

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)***Clause 7.4*

Add the following new requirements and note at the end of this clause (below Figure 9):

- [V2G20-3006] [MCS]** In case of MCS and MCS_BPT: If the EVCC sent the message SessionStopReq with parameter ChargingSession equal to "Pause" it shall pause the Data-Link (D-LINK_PAUSE.request()) after receiving the message SessionStopRes with ResponseCode set to "OK" and follow the sleep and wake-up requirements defined in ISO 15118-10:202X, 7.6.
- [V2G20-3007] [MCS]** In case of MCS and MCS_BPT: If the SECC received the message SessionStopReq with parameter ChargingSession equal to "Pause" it shall pause the Data-Link (D-LINK_PAUSE.request()) after sending the message SessionStopRes with ResponseCode set to "OK" and follow the sleep and wake-up requirements defined in ISO 15118-10:202X, 7.6.

NOTE 3 Requirements [V2G20-1227] and [V2G20-1777] are not applicable for MCS and MCS_BPT.

Clause 7.5

Replace second sentence of the first paragraph with:

ISO 15118-3, ISO 15118-8, and ISO 15118-10 define additional details on data link layer to be covered.

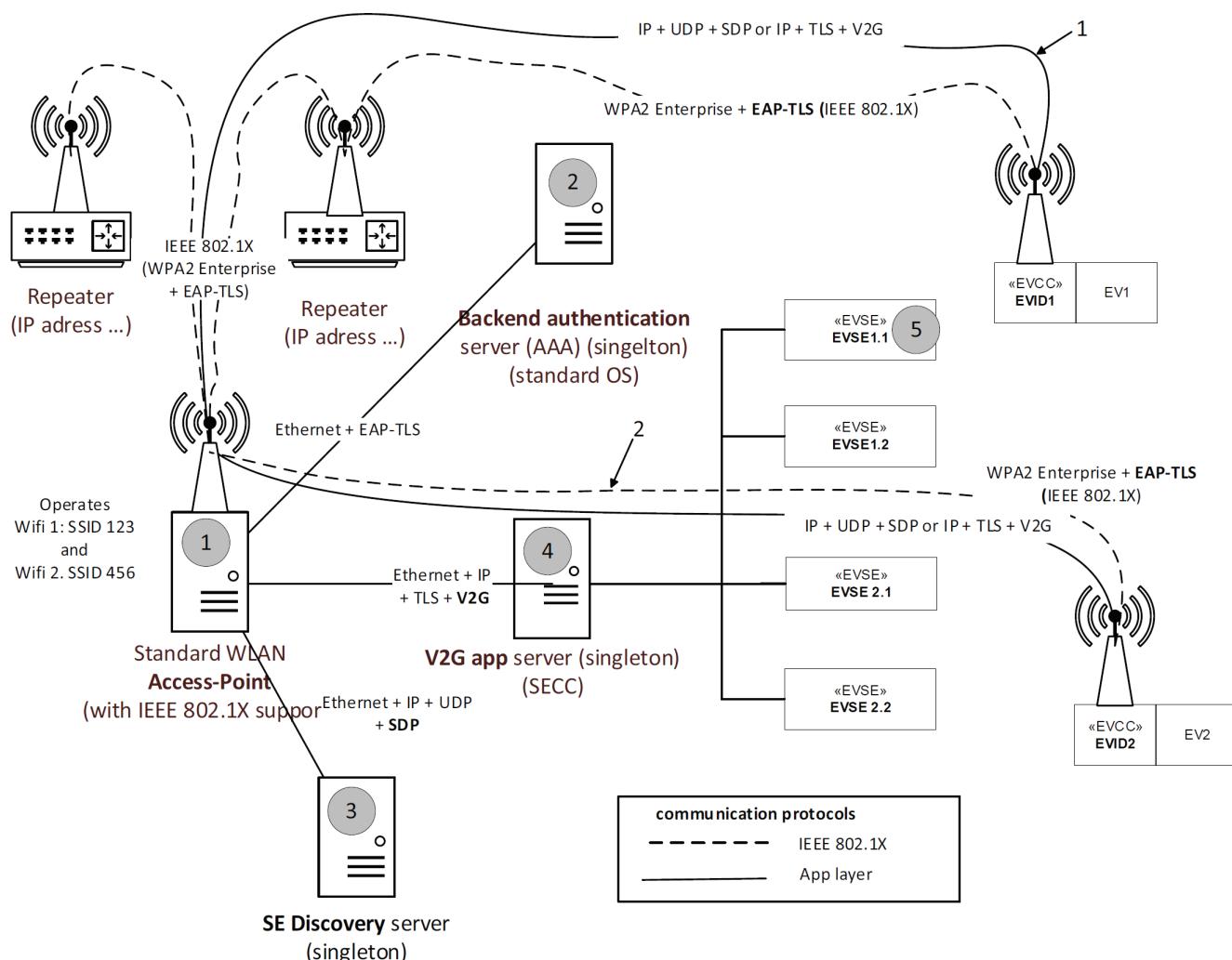
Add the following new requirement above subclause 7.5.1:

- [V2G20-3008] [MCS]** If a V2G entity communicates by 10BASE-T1S, the V2G entity shall comply with ISO 15118-10.

Clause 7.5.1.2

Replace Figure 10 with this figure:

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

**Key**

- 1 App layer communication protocol
- 2 IEEE 802.1X communication protocol

Figure 10 — IEEE 802.1X example with backend authentication for WPT

Add the following new NOTE after NOTE 8 below [V2G20-2368]:

NOTE 9 Although this requirement specifies using RDNs from Issuer field of the root certificates, per IETF RFC 5280, 4.1.2.4 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399) for root certificates these RDNs should be the same between the Issuer field and the Subject field.

Delete the following requirement: [V2G20-2371]

Replace NOTE 21 below [V2G20-1008] with:

NOTE 21 As defined in IETF RFC 6960 (as updated by IETF RFC 8954), an OCSP responder might either be the Sub-CA itself, or it might be an entity which is directly signed by the corresponding Sub-CA/Root CA using a key pair with a special extended key usage flag in the certificate.

Add the following new NOTE after NOTE 29 below [V2G20-2403]:

NOTE 30 Although this requirement specifies using RDNs from Issuer field of the root certificates, per IETF RFC 5280, 4.1.2.4 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399) for root certificates these RDNs should be the same between the Issuer field and the Subject field.

Renumber all NOTES starting from the original NOTE 9.

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)***Clause 7.7.3.10*

Add the following new requirements and note at the end of clause 7.7.3.10:

[V2G20-3009] [MCS] Backwards compatibility with ISO 15118-2 shall not be implemented for an EVCC using MCS.

[V2G20-3010] [MCS] Backwards compatibility with ISO 15118-2 shall not be implemented for a SECC using MCS.

NOTE 10 Requirements [V2G20-2054] through [V2G20-2070] are not applicable for MCS and MCS_BPT.

Clause 7.8.3.1, Table 14

In Table 14: Replace the table row with payload type value 0x8007 - 0x8100 with the following new rows:

Payload type value	Payload type identifier	Explanation
0x8007 - 0x8009	Not applicable	Reserved for future use
0x8010	Part20ACDERMainstreamPayloadID	EXI encoded V2G messages of this document which are exchanged as part of the main stream of the communication flow and are specific to AC BPT DER. This set of messages is using the XSD schema with the namespace "urn:iso:std:iso:15118:-20:AC-DER". Refer to Annex L for the definition of this message set.
0x8011 - 0x8100	Not applicable	Reserved for future use

Clause 7.9.1.3

Add the following new requirement below requirement [V2G20-5125]:

[V2G20-3011] [DER] The XML schema with the namespace "urn:iso:std:iso:15118:-20:AC-DER" shall be used for encoding and decoding EXI streams sent or received with Part20ACDER-MainstreamPayloadID and defined in Annex L.

Clause 7.9.2.4.2

Replace the text below the requirement [V2G20-2476] with the following text:

[V2G20-3012] NIST FIPS PUB 202 defines SHAKE256 as an extendable-output function (XOF). Hence the output length of SHAKE256 (referred as 'd' by NIST FIPS PUB 202) can be configured to any necessary value as needed by the application. For signatures as defined by [V2G20-2476], the output length 'd' of SHAKE256 shall be 114 bytes (912 bits).

NOTE 2 IETF RFC 8032, 5.2 specifies using 114 bytes (912 bits) as the output length of SHAKE256. This requirement keeps the SHAKE256 output length consistent between the IETF RFC 8032 and this document.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

[V2G20-771] The following message elements of the XML signature framework shall not be used when transmitting signatures in the header of the V2G message:

- Id (attribute in SignedInfo)
- ##any in SignedInfo – CanonicalizationMethod
- HMACOutputLength in SignedInfo – SignatureMethod
- ##other in SignedInfo – SignatureMethod
- Type (attribute in SignedInfo-Reference)
- ##other in SignedInfo – Reference – Transforms – Transform
- XPath in SignedInfo – Reference – Transforms – Transform
- ##other in SignedInfo – Reference – DigestMethod
- Id (attribute in SignatureValue)
- Object (in Signature)
- KeyInfo

NOTE 3 This allows to determine an upper bound for the size of the signature header.

For the application of XMLDSig, any element which should be signed is addressable. In this document, this is achieved by a URI referencing the ID attribute of such an element. Therefore, any message element that is signed carries an ID attribute. If a specific element is to be signed in all use cases, the ID attribute is marked mandatory in the XSD. Otherwise, if it is signed in only some use cases, the ID attribute is marked optional and can be omitted when not needed.

NOTE 4 Presence of an ID attribute does not necessarily indicate that a signature is used, i.e. if no signature is used, an ID can be present nevertheless.

NOTE 5 Refer IETF RFC 3986 as updated by IETF RFC 6874 and IETF RFC 7320 for details of URI.

Clause 7.9.2.4.3

Replace Table 17 with this table:

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table 17 — Overview of applied XML based signatures

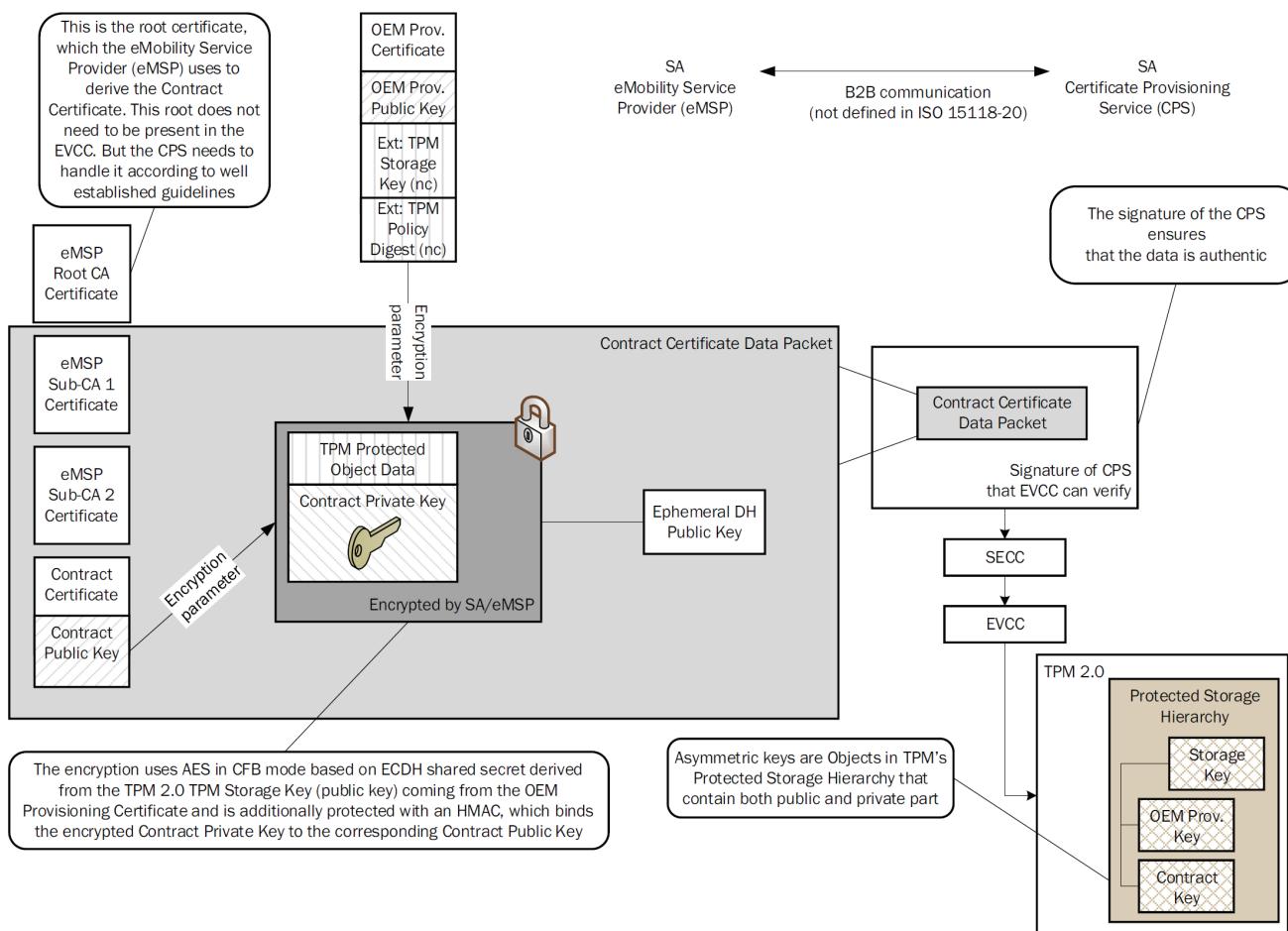
XML message	Protected fields	Signing entity (sender)	Verifying entity (receiver)
AuthorizationReq	PnC_AReqIdentificationMode	EVCC; signed with private key associated with the contract certificate provided within PnC_AReqAuthorizationMode	SECC
CertificateInstallationReq	OEMProvisioningCertificateChain	EVCC; signed with private key associated with OEM provision certificate (transmitted in message body element)	secondary actor
CertificateInstallationRes	SignedInstallationData	secondary actor; signed with the private key associated with the leaf certificate of the certificate provisioning service	EVCC
MeteringConfirmationReq	SignedMeteringData	EVCC; signed with private key associated with the contract certificate (certificate is transmitted in AuthorizationReq message)	SECC
ScheduleExchangeRes	AbsolutePriceSchedule + PriceLevelSchedule	secondary actor; signed with the private key associated with the eMSP Sub-CA2 certificate	EVCC

Replace NOTE 1 below the requirement [V2G20-2479] with:

NOTE 1 The key in the ‘value’ field of ‘generalName’ parameter of ‘accessLocation’ field of ‘accessDescription’ (x448PublicKey) parameter in the extension ‘subjectInfoAccess’ is encoded for use only in ECDH algorithm. It is not possible to use it to verify signatures using the Ed448 algorithm.

Clause 7.9.2.5.3, Figure 25

Replace Figure 25 with this figure:

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Figure 25 — Process for CertificateInstallationRes for EVCC equipped with TPM 2.0***Clause 7.9.2.5.3.3, Figure 26*

Replace Figure 26 with this figure:

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

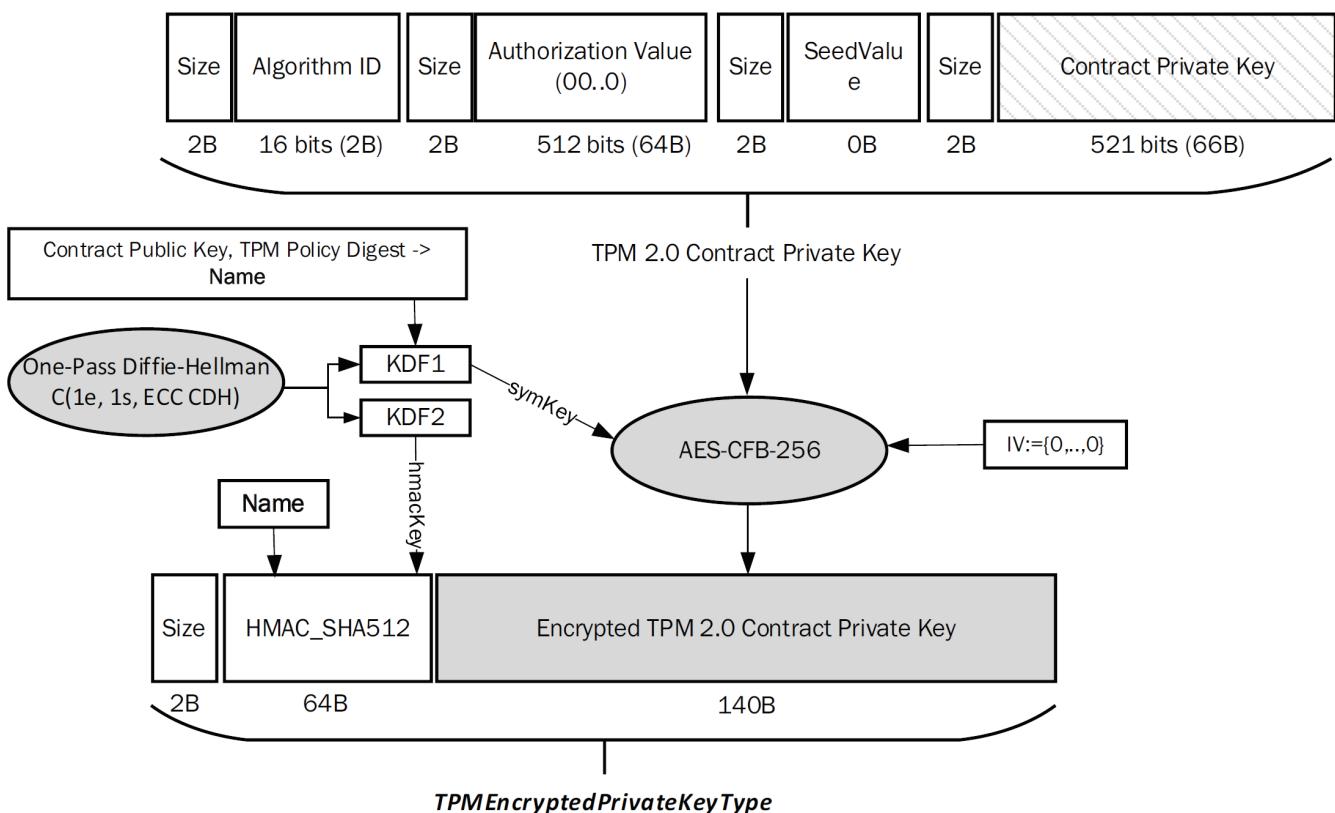


Figure 26 — Contract key encryption for direct import into EVCC's TPM 2.0 (for (elliptic curve) EC P-521/secp521r1)

Clause 7.9.2.5.4

Replace requirement [V2G20-2530] and NOTE 5 with:

- [V2G20-3013]** When the mechanism defined by [V2G20-2320] indicates usage of the (elliptic curve) EC as specified by [V2G20-2319], the “Contract Transport Public Key” of the OEM provisioning certificate shall be used as static public key for calculation of the session key as defined by [V2G20-2535].

NOTE 5 Refer to B.7.2 for further details of “Contract Transport Public Key” stored in the ‘value’ field of ‘generalName’ parameter of ‘accessLocation’ field of ‘accessDescription (x448PublicKey)’ parameter in the extension ‘subjectInfoAccess’ of the OEM provisioning certificate.

Replace requirement [V2G20-2534] and NOTE 9 with:

- [V2G20-3014]** If the EVCC receives the parameter ECDHCurve set to ‘X448’, it shall use the private key associated with the “Contract Transport Public Key” of the OEM Provisioning Certificate along with the public key calculated from [V2G20-2532] for calculation of the session key as defined by [V2G20-2535].

NOTE 9 Refer to B.7.2 for the OEM provisioning certificate profile associated with the algorithm specified by [V2G20-2319] and [V2G20-2674]. Refer to for further details of the xx448 private key.

Clause 7.10.1.1

Add the following new requirements and note at the end of the section (above 7.10.1.2):

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

- [V2G20-3015] [MCS]** If 10BASE-T1S communication according to ISO 15118-10 is applied, the SDP client in the EVCC shall use SECC discovery message with the payload type SDPRequestPayloadID (see Table 14).
- [V2G20-3016] [MCS]** If 10BASE-T1S communication according to ISO 15118-10 is applied, the SDP client in the EVCC shall only accept SDP response messages with the payload type SDPResponsePayloadID (see Table 14).
- [V2G20-3017] [MCS]** If the SDP server shall handle charging services with 10BASE-T1S (according to ISO 15118-10), the SDP server shall accept SECC discovery request messages with payload type SDPRequestPayloadID (see Table 14).
- [V2G20-3018] [MCS]** An SDP server which is used for 10BASE-T1S communication according to ISO 15118-10 shall use SECC discovery response message for 10BASE-T1S with payload type SDPResponsePayloadID (see Table 14).

NOTE 1 Requirements [V2G20-2273] through [V2G20-2280] are not applicable for MCS and MCS_BPT.

Clause 7.10.1.5

Replace title of clause 7.10.1.5 with:

SECC discovery request message for communication according to ISO 15118-3 or ISO 15118-10

Add the following new requirement at the end of the section (above 7.10.1.6):

- [V2G20-3019] [MCS]** For communication according to ISO 15118-10, an SDP client shall send SECC discovery request messages with the security option value equal to 0x00, equivalent to secured with TLS.

Clause 7.10.1.6

Replace title of clause 7.10.1.6 with:

SECC discovery response message for communication according to ISO 15118-3 or ISO 15118-10*Clause 8.2.1*

Add the following requirement below requirement [V2G20-1039]:

- [V2G20-3020] [DER]** If an EVCC supports the service AC DER and intends to use it for this V2G communication session, it shall add an AppProtocol element to the supportedAppProtocolReq with ProtocolNamespace set to "urn:iso:std:iso:15118:-20:AC-DER", VersionNumberMajor set to "1" and VersionNumberMinor set to "0".

Add the following requirement below requirement [V2G20-5126]:

- [V2G20-3021] [MCS]** If an EVCC supports the service MCS and intends to offer it for this V2G communication session, it shall add an AppProtocol element to the supportedAppProtocolReq with ProtocolNamespace set to "urn:iso:std:iso:15118:-20:DC", VersionNumberMajor set to "1" and VersionNumberMinor set to "0".

Clause 8.3.4

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Add the following new clauses below 8.3.4.8:

8.3.4.9 MCS messages

- [V2G20-3022] [MCS]** If the MCS or MCS_BPT service is selected, the EVCC and the SECC shall implement the DC messages as specified in 8.3.4.5.

8.3.4.10 AC DER messages

- [V2G20-3023] [DER]** If the AC DER service is selected, the EVCC and the SECC shall implement the AC DER messages as specified in L.2.1.1.

Clause 8.3.4.1.2

Replace Note 5 with:

NOTE 5 In case of communication according to ISO 15118-3, from first authorization until termination of the V2G communication session or physical plug out. A physical plug out is indicated by a CP state change B to A for conductive charging based on IEC 61851-1, and by CE state changes from state B/B_Aux to A for conductive charging according to IEC 61851-23-3.

Clause 8.3.5

Add the following new clauses below 8.3.5.7:

8.3.5.8 MCS

- [V2G20-3024] [MCS]** If the MCS or MCS_BPT service is selected, the EVCC and the SECC shall implement the complex data types of the DC message set as specified in 8.3.5.5.

8.3.5.9 AC DER

- [V2G20-3025] [DER]** If the AC DER service is selected, the EVCC and the SECC shall implement the complex data types, physical values and simple data types as specified in L.2.2.1 and L.2.2.2.

Clause 8.4.3.1

In Table 204: Replace the table row with ServiceID (unsignedShort) value 8-64 with the following new rows:

ServiceID (unsignedShort)	ServiceName	Description
8	MCS	MCS energy transfer, physical layer according to ISO 15118-10
9	MCS_BPT	MCS energy transfer with BPT, physical layer according to ISO 15118-10
10	AC_DER	AC Charging with BPT, EV being responsible for acting as a DER and fulfilling a dedicated part of the grid codes requirements defined for the BPT system consisting of an EV and a permanently connected EV supply equipment.
11-64		Reserved by this document

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Add the following new requirements at the end of the subclause (above 8.4.3.2):

- [V2G20-3026] [MCS]** If the service with the ServiceName = MCS or MCS_BPT was selected by the EVCC and confirmed by the SECC, the respective requirements in Annex K shall be applied.
- [V2G20-3027] [DER]** If the service with the ServiceName = AC_DER was selected by the EVCC and confirmed by the SECC, all requirements in Annex L shall be applied.
- [V2G20-3028] [DER]** If the AC DER service shall be supported by the SECC, the SECC shall support and offer ServiceRenegotiation, i.e., the SECC shall set ServiceRenegotiationSupported = TRUE in the ServiceDiscoveryRes.
- [V2G20-3029] [DER]** If the AC DER service shall be supported by the EVCC, the EVCC shall support ServiceRenegotiation and execute it, if requested to do so by the SECC.
- [V2G20-3030] [DER]** If the service with the ServiceName = AC_DER was selected by the EVCC and confirmed by the SECC, all requirements applicable to the service with ServiceName = AC shall apply as well.

Clause 8.4.3.2

Add the following new clauses below 8.4.3.2.7:

8.4.3.2.8 MCS service

- [V2G20-3031] [MCS]** If the MCS service is selected, the EVCC and the SECC shall implement the MCS service parameters as specified in K.3.1.1.2.

8.4.3.2.8.1 MCS BPT service

- [V2G20-3032] [MCS]** If the MCS_BPT service is selected, the EVCC and the SECC shall implement the MCS_BPT service parameters as specified in K.3.1.1.2.1.

8.4.3.2.9 AC DER service

- [V2G20-3033] [DER]** If the AC DER service is selected, the EVCC and the SECC shall implement the AC DER service parameters as specified in L.3.1.1.2.

Clause 8.5

Replace the title of 8.5.6 with:

V2G message synchronization for AC, AC DER and DC with IEC 61851-1 signalling

Add the following new clauses below 8.5.7:

8.5.8 V2G message synchronization for MCS with IEC 61851-23-3 signalling

- [V2G20-3034] [MCS]** If the MCS or MCS_BPT service is selected, the EVCC and the SECC shall implement the requirements specified in K.4.3.

Clause 8.5.2

Replace the first sentence of NOTE 3 with:

This document supports PLC, WiFi and 10BASE-T1S communication.

- **Entwurf** -

E DIN EN ISO 15118-20/A1:2025-02 ISO 15118-20:2022/DAM 1:2024(en)

Clause 8.6.3.2

Add the following new text at the beginning of the clause:

The following requirements apply for the services AC, AC_BPT and AC_DER.

Clause 8.6.3.3

Add the following new text at the beginning of the clause:

The following requirements apply for the services DC, DC_BPT, MCS and MCS_BPT.

Clause 8.6.4.2

Add the following new text at the beginning of the clause:

The following requirements apply for the services AC, AC_BPT and AC_DER.

Clause 8.6.4.3

Add the following new text at the beginning of the clause:

The following requirements apply for the services DC and DC_BPT. The requirements for the services MCS and MCS_BPT are specified in K.5.2.1.

Clause 8.6.4.5.3.2

Add the following new text at the beginning of the clause:

The following requirements apply for the services AC, AC_BPT and AC_DER.

Clause 8.6.4.5.3.3

Add the following new text at the beginning of the clause:

The following requirements apply for the services DC and DC_BPT. The requirements for the services MCS and MCS_BPT are specified in K.5.2.2.1.1.

Clause 8.6.4.6.3.2

Add the following new text at the beginning of the clause:

The following requirements apply for the services AC, AC_BPT and AC_DER.

Clause 8.6.4.6.3.3

Add the following new text at the beginning of the clause:

The following requirements apply for the services DC and DC_BPT. The requirements for the services MCS and MCS_BPT are specified in K.5.2.3.1.1.

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)*****Annex A***

Add a bullet point with the following text and link below the bullet point "V2G_CI_AC":

- "V2G_CI_AC_DER": Defines the messages exclusively used for the AC DER service. The XSD file can be downloaded from:
https://standards.iso.org/iso/15118/-20/ed-1/Amd1/en/V2G_CI_AC_DER.xsd

Clause B.1

Replace the entire text below Table B.1 with the following text:

NOTE 1 The following OIDs apply (ASN.1 notation):

- { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }
- { iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) 1 }
- { iso(1) identified-organization(3) certicom(132) curve(0) 35 }
- { iso(1) identified-organization(3) thawte(101) id-EdDSA448(113) }
- { iso(1) identified-organization(3) thawte(101) id-X448(111) }
- { joint-iso-itu-t(2) ds(5) attributeType(4) countryName(6) }
- { joint-iso-itu-t(2) ds(5) attributeType(4) organizationName(10) }
- { joint-iso-itu-t(2) ds(5) attributeType(4) organizationalUnitName(11) }
- { joint-iso-itu-t(2) ds(5) attributeType(4) commonName(3) }
- { itu-t(0) data(9) pss(2342) ucl(19200300) pilot(100) pilotAttributeType(1) domainComponent(25) }
- { joint-iso-itu-t(2) ds(5) certificateExtension(29) subjectKeyIdentifier(14) }
- { joint-iso-itu-t(2) ds(5) certificateExtension(29) keyUsage(15) }
- { joint-iso-itu-t(2) ds(5) certificateExtension(29) basicConstraints(19) }
- { joint-iso-itu-t(2) ds(5) certificateExtension(29) cRLNumber(20) }
- { joint-iso-itu-t(2) ds(5) certificateExtension(29) deltaCRLIndicator(27) }
- { joint-iso-itu-t(2) ds(5) certificateExtension(29) issuingDistributionPoint(28) }
- { joint-iso-itu-t(2) ds(5) certificateExtension(29) cRLDistributionPoints(31) }
- { joint-iso-itu-t(2) ds(5) certificateExtension(29) authorityKeyIdentifier(35) }
- { joint-iso-itu-t(2) ds(5) certificateExtension(29) extKeyUsage(37) }
- { joint-iso-itu-t(2) ds(5) certificateExtension(29) freshestCRL(46) }
- { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithms(4) hashalgs(2) sha512(3) }

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

- { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithms(4) hashalgs(2) shake256-len(18) }
- { iso(1) standard(0) 15118 part20(20) extensions(0) contractOperatorName(1) }
- { iso(1) standard(0) 15118 part20(20) extensions(0) contractTariffName(2) }
- { iso(1) standard(0) 15118 part20(20) extensions(0) contractDynamicInformationUrl(3) }
- { iso(1) standard(0) 15118 part20(20) extensions(0) tpmStorageKey(4) }
- { iso(1) standard(0) 15118 part20(20) extensions(0) tpmPolicyDigest(5) }
- { iso(1) standard(0) 15118 part20(20) extensions(0) crossCertIndication(6) }
- { iso(1) standard(0) 15118 part20(20) extensions(0) utf8String(7) }
- { iso(1) standard(0) 15118 part20(20) extensions(0) octetString(8) }
- { iso(1) standard(0) 15118 part20(20) extensions(0) x448PublicKey(9) }
- { iso(1) standard(0) 15118 part20(20) extensions(0) bitString(10) }
- { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) pe(1) authorityInfoAccess(1) }
- { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) pe(1) subjectInfoAccess(11) }
- { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) kp(3) id-kp-serverAuth(1) }
- { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) kp(3) id-kp-clientAuth(2) }
- { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) kp(3) id-kp-OCSPSigning(9) }
- { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) ocsp(1) }
- { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) id-ad-ocsp(1) id-pkix-ocsp-basic(1) }
- { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) id-ad-ocsp(1) id-pkix-ocsp-nonce(2) }
- { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) id-ad-ocsp(1) id-pkix-ocsp-response(4) }
- { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) id-ad-ocsp(1) id-pkix-ocsp-pref-sig-algs(8) }
- { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) caIssuers(2) }

NOTE 2 The online certificate status protocol (OCSP), defined in IETF RFC 6960 (as updated IETF RFC 8954) is a protocol used for obtaining the revocation status of an X.509 certificate. OCSP is as an alternative to certificate revocation lists (CRL). OCSP is an online service. This means, that a backend infrastructure supports OCSP services in order to be able to use that service.

NOTE 3 Refer to ITU-T X.680 for details of ASN.1 notation.

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

When the certificate status is provided via OCSP services, id-pe-authorityInfoAccess OID is used within the AuthorityInfoAccess extension. The OID repository [99] also refers to id-pe-authorityInfoAccess as authorityInfoAccess(1) (see NOTE 1 above providing the OID value for id-pe-authorityInfoAccess).

Within a x.509 certificate, the id-ad-ocsp OID is used within the AuthorityInfoAccess extension as accessMethod if revocation information for the certificate containing this extension is available using the online certificate status protocol (OCSP). When id-ad-ocsp appears as accessMethod, the accessLocation field is the location of the OCSP responder, using the conventions defined IETF RFC 6960 as updated IETF RFC 8954.

id-ad-ocsp is also known as id-pkix-ocsp. The OID repository [99] also refers to id-ad-ocsp as ocsp(1) (see NOTE 1 above providing the OID value for id-ad-ocsp).

If the certificate status is provided via a certificate revocation list (CRL), id-ce-cRLDistributionPoints OID is used within the CRLDistributionPoints extension. The OID repository [99] also refers to id-ce-cRLDistributionPoints as cRLDistributionPoints(31) (see NOTE 1 above providing the OID value for id-ce-cRLDistributionPoints).

The OID for 'ecdsa-with-SHA512' is defined as { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 } in ASN.1 notation (refer to ITU-T X.680 for details of ASN.1 notation).

The OID for 'id-ecPublicKey' is defined as { iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) 1 } in ASN.1 notation (refer to ITU-T X.680 for details of ASN.1 notation).

The OID for 'secp521r1' is defined as { iso(1) identified-organization(3) certicom(132) curve(0) 35 } in ASN.1 notation (refer to ITU-T X.680 for details of ASN.1 notation).

When subject information access is provided, id-pe-subjectInfoAccess OID is used within the subjectInfoAccess extension. The OID repository [99] also refers to id-pe-subjectInfoAccess as subjectInfoAccess(11) (see NOTE 1 above providing the OID value for id-pe-subjectInfoAccess).

The OID repository [99] provides the EdDSA448 algorithm identifier as id-EdDSA448 while the IETF RFC 8410 provides the identifier as id-Ed448. Both OID values are actually same and as such these identifiers can be used interchangeably (see NOTE 1 above providing the OID value for id-EdDSA448).

The OID repository [99] also refers to id-at-countryName as countryName(6) (see NOTE 1 above providing the OID value for countryName).

The OID repository [99] also refers to id-at-organizationName as organizationName(10) (see NOTE 1 above providing the OID value for organizationName).

The OID repository [99] also refers to id-at-organizationalUnitName as organizationalUnitName(11) (see NOTE 1 above providing the OID value for organizationalUnitName).

The OID repository [99] also refers to id-at-commonName as commonName(3) (see NOTE 1 above providing the OID value for commonName).

The OID repository [99] also refers to id-domainComponent as domainComponent(25) (see NOTE 1 above providing the OID value for domainComponent).

The OID repository [99] also refers to id-ce-subjectKeyIdentifier as subjectKeyIdentifier(14) (see NOTE 1 above providing the OID value for id-ce-subjectKeyIdentifier).

The OID repository [99] also refers to id-ce-keyUsage as keyUsage(15) (see NOTE 1 above providing the OID value for id-ce-keyUsage).

The OID repository [99] also refers to id-ce-basicConstraints as basicConstraints(19) (see NOTE 1 above providing the OID value for id-ce-basicConstraints).

The OID repository [99] also refers to id-ce-cRLNumber as cRLNumber(20) (see NOTE 1 above providing the OID value for id-ce-cRLNumber).

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

The OID repository [99] also refers to id-ce-deltaCRLIndicator as deltaCRLIndicator(27) (see NOTE 1 above providing the OID value for id-ce-deltaCRLIndicator).

The OID repository [99] also refers to id-ce-issuingDistributionPoint as issuingDistributionPoint(28) (see NOTE 1 above providing the OID value for id-ce-issuingDistributionPoint).

The OID repository [99] also refers to id-ce-authorityKeyIdentifier as authorityKeyIdentifier(35) (see NOTE 1 above providing the OID value for id-ce-authorityKeyIdentifier).

The OID repository [99] also refers to id-ce-extKeyUsage as extKeyUsage(37) (see NOTE 1 above providing the OID value for id-ce-extKeyUsage).

The OID repository [99] also refers to id-ce-freshestCRL as freshestCRL(46) (see NOTE 1 above providing the OID value for id-ce-freshestCRL).

The OID repository [99] also refers to id-sha512 as sha512(3) (see NOTE 1 above providing the OID value for id-sha512).

The OID repository [99] also refers to id-shake256-len as shake256-len(18) (see NOTE 1 above providing the OID value for id-shake256-len).

The OID repository [99] also refers to id-contractOperatorName as contractOperatorName(1) (see NOTE 1 above providing the OID value for contractOperatorName).

The OID repository [99] also refers to id-contractTariffName as contractTariffName(2) (see NOTE 1 above providing the OID value for contractTariffName).

The OID repository [99] also refers to id-contractDynamicInformationUrl as contractDynamicInformationUrl(3) (see NOTE 1 above providing the OID value for contractDynamicInformationUrl).

The OID repository [99] also refers to id-tpmStorageKey as tpmStorageKey(4) (see NOTE 1 above providing the OID value for tpmStorageKey).

The OID repository [99] also refers to id-tpmPolicyDigest as tpmPolicyDigest(5) (see NOTE 1 above providing the OID value for tpmPolicyDigest).

The OID repository [99] also refers to id-crossCertIndication as crossCertIndication(6) (see NOTE 1 above providing the OID value for crossCertIndication).

The OID repository [99] also refers to id-utf8String as utf8String(7) (see NOTE 1 above providing the OID value for utf8String).

The OID repository [99] also refers to id-octetString as octetString(8) (see NOTE 1 above providing the OID value for octetString).

The OID repository [99] also refers to id-x448PublicKey as x448PublicKey(9) (see NOTE 1 above providing the OID value for x448PublicKey).

The OID repository [99] also refers to id-bitString as bitString(10) (see NOTE 1 above providing the OID value for bitString).

The OID repository [99] also refers to id-ad-caIssuers as caIssuers(2) (see NOTE 1 above providing the OID value for id-ad-caIssuers).

It should be noted that although the certificate validity of each certificate type will be as per the definition in this Annex, the certificate validity remaining at the time of V2G entity production or deployment may be less than the requirements as specified in this Annex. This is because the certificate may have been generated long before the V2G entity was produced and/or deployed.

Furthermore, the certificate validity is not directly related to the date of issuance of a certificate but is rather tied to 'notBefore' and 'notAfter' fields of the certificate.

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

For example, if a V2G Root CA Certificate has a 'notBefore' field of 20100301180000Z (March 1 18:00:00 2010 GMT) and a 'notAfter' field of 20350301175959Z (March 1 17:59:59 2035 GMT), this results in a validity of 25 years. If a vehicle manufactured in March 2020 uses that V2G Root CA Certificate, that root certificate will only have 15 more years of validity left before the certificate expires.

Clause B.2

Add the following new requirements and notes above requirement [V2G20-2685]:

[V2G20-3035] All certificates used for any purposes defined by this document shall meet all requirements as specified by this document, IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399) and ITU-T X.509.

NOTE 1 Per [V2G20-1001], all certificate validations will also be done per IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399). [V2G20-3035] complements [V2G20-1001].

NOTE 2 IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399) specifies maximum allowed length for various parameters in the certificates. Implementations should be cognizant of this. Unless specified otherwise, [V2G20-3035] limits implementations conforming to this document from exceeding these restrictions.

NOTE 3 In some cases, IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399) specifies the length restrictions in appendices. For example, Appendix A of IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399) limits maximum length of Organization Name to 64 characters. This is just one example. Refer to IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399), including the appendices, for complete list of length limits.

[V2G20-3036] In case of conflicts between certificate requirements as specified by this document and IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399) and/or ITU-T X.509, requirements specified by this document shall be given higher precedence.

[V2G20-3037] In case of conflicts between certificate requirements as specified by IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399) and ITU-T X.509, requirements specified by IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399) shall be given higher precedence.

Add the following new paragraph below requirement [V2G20-2686]:

Certificate extensions are used to provide additional information about the certificates, specify constraints on the key usage, provide information about revocation services, etc. Each extension contains an extnID field which is the unique OID identifying the extension, a Boolean critical field used to indicate whether the extension is critical or not and an extnValue field in octet string format containing the DER encoding of the ASN.1 value of the extension. The certificate profiles defined by this annex specify the values for various parameters or elements contained within each extension in ASN.1 structure before the DER encoding.

Clause B.2.2

Add the following new paragraph below the second paragraph:

It should be noted that certain certificate extensions may be marked as critical or non-critical simply so that the certificate profile can match the requirements specified by IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399) and hence the certificates may be processed by most commonly available TLS implementations. In such cases, requirements below the certificates will indicate whether the relying parties are required to process or not process those extensions.

Replace the last paragraph with:

Similarly, some requirements in this document may mandate the relying party/validating entity to process certain critical/non-critical extensions if they are present. Those requirements will make it clear when

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Printed copies are uncontrolled
 the relying party is mandated to process the extensions and which exact extensions are mandated to be processed.

Clause B.2.3

Replace requirement [V2G20-2696] with:

- [V2G20-2696]** Each relying party shall be capable of interpreting and processing 'AuthorityKeyIdentifier', 'SubjectKeyIdentifier', 'ExtendedKeyUsage', 'CRLDistributionPoints', 'AuthorityInfoAccess' and 'SubjectInfoAccess' extensions.

Add the following text below requirement [V2G20-2696]:

All certificate profiles defined by this Annex identify 'AuthorityKeyIdentifier' and 'SubjectKeyIdentifier' extensions as non-critical. Relying parties are not required to process these extensions. It is left to the local policy of the relying parties whether they need to process 'AuthorityKeyIdentifier' and 'SubjectKeyIdentifier' extensions or not.

Replace the text below requirement [V2G20-2582] until the end of clause B.2.3 with the following text:

Per IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399), if 'AuthorityInfoAccess' is present, 'accessMethod' and 'accessLocation' that are part of 'AuthorityInfoAccess' are also present. If 'accessMethod' and 'accessLocation' are not present while 'AuthorityInfoAccess' is present, the relying party will reject the certificate.

Per IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399), if 'SubjectInfoAccess' is present, 'accessMethod' and 'accessLocation' that are part of 'SubjectInfoAccess' are also present. If 'accessMethod' and 'accessLocation' are not present while 'SubjectInfoAccess' is present, the relying party will reject the certificate.

Certain parameters in the certificate profiles specified by this annex utilize UTF8 format. Relying parties should be capable of processing UTF8 characters as specified by ISO/IEC 10646.

NOTE 3 It should be noted that each character in UTF8 format can be upto 4 bytes long. Hence a 64 character UTF8 field can take upto 256 bytes.

- [V2G20-1224]** The Distinguished Name (DN) shall be represented as a string that complies with IETF RFC 4514, Clause 3.

Certificate Issuer and Subject fields contain DNs that are used to identify the certificate path. A DN is made up of multiple Relative Distinguished Names (RDNs). Each RDN contains AttributeType and AttributeValue. AttributeType determines the type of the RDN (using OIDs as called out in B.1) while AttributeValue contains the actual value of the RDN. In some cases, the type of the data contained within the AttributeValue is determined by (or encoded in) AttributeType; in others, that information is designated by DirectoryString.

- [V2G20-3038]** Unless specified otherwise, either by this document or by IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399), all RDNs shall utilize UTF8 format.

NOTE 4 For example, IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399) states that the 'Country' RDN should be in 'PrintableString' format. In that case, [V2G20-3038] allows usage of format as specified by IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399), while for 'Organization' which is allowed to utilize multiple formats per IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399), [V2G20-3038] limits the format to UTF8.

IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399) also specifies the length of data allowed in certain certificate fields, including the RDNs. Unless specified otherwise, certificates used for ISO 15118-20 will follow the length requirements as specified by IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399).

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Printed copies are uncontrolled

pathLenConstraint parameter of BasicConstraints extension defines the maximum number of possible Sub-CA(s) below the certificate currently being processed. It does not, however, mean that it is necessary to have that many Sub-CA(s) below the certificate currently being processed. As long as the chosen implementation does not violate any requirements specified by this document, it is left to the discretion of the implementers how many Sub-CA(s) they implement/support and the certificate structure they choose.

Add the following new subclauses at the end of B.2.3:

B.2.3.1 Certificate policy requirements for all certificate profiles

Certificate policies provide the set of rules, terms, and conditions under which the certificates are being generated by the CA. They may also indicate the intended use of the certificates. Relying parties often rely on certificate policies to ensure that the certificate meets the security and business needs of the relying party.

Most profiles make ‘certificatePolicies’ extension optional and non-critical. They also indicate that processing of ‘certificatePolicies’ extension is not mandatory and is left to the local policy of the relying party.

Per IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399), any certificate policy that is present in any certificate in a given certificate chain should be valid for the entire certification path. This means that if the ‘certificatePolicies’ extension is present in any certificate in a certificate chain, the ‘certificatePolicies’ extension should appear in all certificates in that certificate chain except the root certificate.

Certificate policy is provided in the certificates using the OIDs. Hence, per IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399), the certificate policy OID provided in a leaf certificate should also appear in the Sub CA1 (if present) and Sub CA2 certificates to be valid for the entire certification path.

For example, if the ‘certificatePolicies’ extension is missing from Sub CA1 certificate, no explicit certificate policies are allowed below that CA certificate.

‘certificatePolicies’ extension should not appear in root certificates as ‘certificatePolicies’ is implicitly set to ‘anyPolicy’ in the root certificate. If the ‘certificatePolicies’ extension were to be present in a root certificate, any updates/changes/modification to the policies would require generating a new root certificate.

Each certificate can conform to multiple certificate policies. In case a particular certificate in a given certificate chain conforms to multiple certificate policies, it is not necessary that every certificate in that certificate chain conforms to all those certificate policies. But the policy that needs to be applied to a leaf certificate has to be valid for the entire chain.

For example, if the leaf certificate conforms to certificate policy A and certificate policy B while Sub-CA2 certificate in that chain only conforms to certificate policy B and if the Sub-CA1 certificate in that chain conforms to certificate policy B, the entire certificate chain is assumed to conform to certificate policy B.

In this same example, if Sub-CA1 certificate conforms to certificate policy A, no single certificate policy is valid for the entire chain. Hence, in this example, the entire certificate chain is assumed to conform to neither certificate policy A nor certificate policy B.

[V2G20-3039] A certificate meeting the requirements specified by this document may correspond to one or more certificate policies. This document does not place any restriction on the number of certificate policies a certificate can conform to.

‘certificatePolicies’ extension is a sequence of ‘PolicyInformation’ fields. Each ‘PolicyInformation’ field provides information regarding one of the certificate policies that the certificate conforms to. In accordance with **[V2G20-3039]**, the number of ‘PolicyInformation’ fields in ‘certificatePolicies’ extension is unrestricted.

The CA is allowed to provide optional qualifying information regarding the certificate policy. For this purpose, each ‘PolicyInformation’ field is allowed to contain an optional ‘policyQualifiers’ parameter.

[V2G20-3040] This document does not mandate inclusion of policy qualifiers in ‘PolicyInformation’ field in ‘certificatePolicies’ extension of the certificate.

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Per IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399), 'policyQualifiers' parameter is a sequence of 'PolicyQualifierInfo' fields. Each 'PolicyQualifierInfo' field provides further information that the CA may like to disseminate regarding the associated certificate policy.

- [V2G20-3041]** This document limits the number of policy qualifiers 'PolicyQualifierInfo' fields to one (1) per certificate policy.

NOTE 1 Per [V2G20-3040], a CA is not required to include 'PolicyQualifierInfo' field in 'PolicyInformation' field in 'certificatePolicies' extension of the certificate. But, if the CA does want to include 'PolicyQualifierInfo' field in 'PolicyInformation' field in 'certificatePolicies' extension of the certificate, per [V2G20-3041], it can only include one per certificate policy.

'PolicyQualifierInfo' is a sequence of two (2) parameters, 'policyQualifierId' and 'qualifier'. 'policyQualifierId' contains the OID identifying the 'qualifier'.

- [V2G20-3042]** When the 'qualifier' parameter in 'PolicyQualifierInfo' field in 'PolicyInformation' field in 'certificatePolicies' extension is set to 'CPSuri' by the CA generating a certificate, that CA shall set 'CPSuri' to the URI of its Certification Practice Statement (CPS) under which the CA is generating the said certificate.

- [V2G20-3043]** The relying parties are not required/mandated by this document to process 'PolicyQualifierInfo' field of 'PolicyInformation' field in 'certificatePolicies' extension. It is left to the local policy of the relying party to define further steps, if any, that the relying party is required to take based on 'CPSuri'.

- [V2G20-3044]** This document prohibits inclusion of user notice policy qualifier in 'PolicyInformation' field in 'certificatePolicies' extension of the certificate.

NOTE 2 This means, that the 'qualifier' parameter in 'PolicyQualifierInfo' field in 'PolicyInformation' field in 'certificatePolicies' extension cannot be set to 'UserNotice' in certificates conforming to this document.

B.2.3.2 Cross certification requirements

- [V2G20-3045]** Cross certification of Root CA(s) shall generate cross certificate(s) meeting the profile described in B.9 (and its subclauses) of this document.

- [V2G20-3046]** Any Sub-CA certificate(s) that is(are) issued to cross certified Sub-CA(s) shall include a cross certification indication. Such certificates shall include a 'SubjectInfoAccess' extension, as defined in IETF RFC 5280, 4.2.2.2, to indicate that the particular certificate is cross certified.

NOTE 1 IETF RFC 5280 has been updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399. These updates are considered to be included in this document.

- [V2G20-3047]** For cross certification indication as specified by **[V2G20-3046]**, 'accessLocation' field of 'SubjectInfoAccess' extension shall be set to "CROSS". [V2G20-2604] and **[V2G20-3077]** shall be used for this purpose.

'SubjectInfoAccess' is defined as a non-critical extension. This document does not require the relying parties relying on and/or processing the Sub-CA certificate(s) to process this extension. It is left to the local policy of the relying party whether it needs to process this extension.

- [V2G20-3048]** Unless specified otherwise, the 'SubjectInfoAccess' extension specified by **[V2G20-3046]** shall contain only one (1) instance of 'accessDescription' field.

This document does not limit the number of cross-certifications. Any cross certification, however, will lead to generation of a new Sub-CA certificate. Refer to H.1.5 and its subclauses for further details on cross-signing.

B.2.3.2.1 End-entity certificate chain selection

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

The end-entities providing their certificates/certificate-chains to the relying parties will need to ensure that they provide a certificate chain containing the right certificates/cross-certified certificates/cross certificates as needed for the particular use case. In most instances, the relying parties will indicate to the end entities the Root Certificate(s) they trust by providing the DNs/RDNs of the trusted Root Certificate(s). The end-entities will need to take this information and use it to find a certificate chain that the relying party would be able to successfully validate for the particular use case.

Different sections of this document provide varying methodologies for relying parties to communicate the DNs/RDNs of the trusted Root Certificate(s). Those methodologies are dependent on the communication technology and other existing outside standards.

Various sections of this document provide use cases for all the different certificates utilized by this document. This annex and its subclauses define the certificate profiles and certificate structure employed for those use cases.

End entities will need to take all this into account as they look for the appropriate certificate chain to provide to the relying party. The process of selection of appropriate end entity certificate chain does not affect security or interoperability. As such this document does not define any algorithm for selection of appropriate end entity certificate chain. The standard, however, does lay out some guidance above to help the end-entities in this endeavor.

Refer to H.1.5 and its subclauses for further details on cross-signing.

Clause B.3.1

Replace Table B.3 with this table:

Table B.3 — V2G Root CA certificate based on curves as defined by [V2G20-2674]

ISO 15118-20 certificate profiles		V2G Root V2G
	Version	x 2 ("2" indicates X.509v3)
	SerialNumber	x
Signature	AlgorithmIdentifier	x
	algorithm	x ecdsa-with-SHA512
	parameters	-
Issuer	Country (C)	(x) (ISO 3166-1 alpha-2 code)
	Organization (O)	x
	Organization Unit (OU)	(x)
	Common Name (CN)	x
	Domain Component (DC)	(x)
Validity	Validity	x [CA discretionary (suggested 25 years)]
	Country (C)	(x) (ISO 3166-1 alpha-2 code)
	Organization (O)	x

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.3 (continued)**

ISO 15118-20 certificate profiles			V2G Root V2G
TbsCertifi- cate	Subject	Organization Unit (OU)	(x)
		Common Name (CN)	x
		Domain Component (DC)	(x)
	SubjectPublicK- eyInfo	AlgorithmIdentifier	x
		algorithm	x id-ecPublicKey
		parameters (ECPa- rameters)	x
		namedCurve	x secp521r1
		SubjectPublicKey	x (BIT STRING)
	IssuerUniqueID		-
	SubjectUniqueID		-
	Extensions	AuthorityKeyIdentifi- er	-
		SubjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier
		keyIdentifier	x (see [V2G20-1852])
		KeyUsage	x / c id-ce-keyUsage
		digitalSignature	0/1
		nonRepudiation (con- tentCommitment)	0/1
		keyEncipherment	0/1
		dataEncipherment	0
		keyAgreement	0/1
		keyCertSign	1
		cRLSign	0
		encipherOnly	0
		decipherOnly	0
		ExtendedKeyUsage	-
		CertificatePolicies	-
		BasicConstraints	x / c id-ce-basicConstraints
		cA	TRUE
		pathLenConstraint	-
		CRLDistribution- Points (CRL)	-
		AuthorityInfoAccess	-

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.3 (continued)**

ISO 15118-20 certificate profiles		V2G Root V2G
SignatureAlgorithm	AlgorithmIdentifier	x
	algorithm	x ecdsa-with-SHA512
	parameters	-
SignatureValue		(Octet-String)

Clause B.3.2

Replace Table B.4 with this table:

Table B.4 — V2G Root CA certificate based on curves as defined by [V2G20-2319]

ISO 15118-20 certificate profiles		V2G Root V2G
TbsCertificate	Version	2 ("2" indicates X.509v3)
	SerialNumber	x
	Signature	AlgorithmIdentifier
		algorithm
		x id-Ed448
	Issuer	parameters
		Country (C) (ISO 3166-1 alpha-2 code)
		x
		(x)
	Subject	Organization (O)
		Organization Unit (OU)
		Common Name (CN)
		Domain Component (DC)
		x (x)
	Validity	Validity [CA discretionary (suggested 25 years)]
	SubjectPublicK-eyInfo	Country (C) (ISO 3166-1 alpha-2 code)
		x
		(x)
		Common Name (CN)
		(x)
	AlgorithmIdentifier	Domain Component (DC)
		x
		(x)
	algorithm	x id-Ed448
	parameters	-
	SubjectPublicKey	x (BIT STRING)

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**
Table B.4 (continued)

ISO 15118-20 certificate profiles		V2G Root V2G
	IssuerUniqueID	-
	SubjectUniqueID	-
Extensions	AuthorityKeyIdentifier	-
	SubjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifierx
	keyIdentifier	x (see [V2G20-1852])
	KeyUsage	x / c id-ce-keyUsage
	digitalSignature	0/1
	nonRepudiation (contentCommitment)	0/1
	keyEncipherment	0/1
	dataEncipherment	0
	keyAgreement	0/1
	keyCertSign	1
	cRLSign	0
	encipherOnly	0
	decipherOnly	0
	ExtendedKeyUsage	-
	CertificatePolicies	-
	BasicConstraints	x / c id-ce-basicConstraints
	cA	TRUE
	pathLenConstraint	-
	CRLDistributionPoints (CRL)	-
	AuthorityInfoAccess	-
SignatureAlgorithm	AlgorithmIdentifier	x
	algorithm	x id-Ed448
	parameters	-
SignatureValue		(Raw BIT STRING)

Clause B.4.1

Replace Table B.5 with this table:

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.5 — Charge point operator certificates based on curves as defined by [V2G20-2674]

ISO 15118-20 certificate profiles		Charge point operator		
		CSO Sub-CA 1 Sub	CSO Sub-CA 2 Sub	SECC Cert Leaf
	Version	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)
	SerialNumber	x	x	x
Signature	AlgorithmIdentifier	x	x	x
	algorithm	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512
	parameters	-	-	-
Issuer	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)
	Common Name (CN)	x	x	x
	Domain Component (DC)	(x)	(x)	(x)
Validity	Validity	x [up to CSO]	x [up to CSO]	x [up to CSO]
Subject	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	x (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)
	Common Name (CN)	x	x	x SECCID (see [V2G20-2583])
	Domain Component (DC)	(x)	(x)	(x) & "CSO"
Subject-PublicKey-Info	AlgorithmIdentifier	x	x	x
	algorithm	x id-ecPublicKey	x id-ecPublicKey	x id-ecPublicKey
	parameters (ECParameters)	x	x	x
	namedCurve	x secp521r1	x secp521r1	x secp521r1
	SubjectPublicKey	x (BIT STRING)	x (BIT STRING)	x (BIT STRING)
IssuerUniqueID		-	-	-
SubjectUniqueID		-	-	-
	AuthorityKeyIdentifier	x / nc id-ce-authorityKeyIdentifier	x / nc id-ce-authorityKeyIdentifier	x / nc id-ce-authorityKeyIdentifier

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**
Table B.5 (continued)

ISO 15118-20 certificate profiles		Charge point operator		
		CSO Sub-CA 1 Sub	CSO Sub-CA 2 Sub	SECC Cert Leaf
TbsCertificate	keyIdentifier	x (see [V2G20-1851])	x (see [V2G20-1851])	x (see [V2G20-1851])
	authorityCertIs- suer	-	-	-
	authorityCertSeri- alNumber	-	-	-
	SubjectKeyIden- tifier	x / nc id-ce-subjectKeyIden- tifier	x / nc id-ce-subjectKey- Identifier	x / nc id-ce-subjectKey- Identifier
	keyIdentifier	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])
	KeyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage
	digitalSignature	0/1	0/1	1
	nonRepudiation (contentCommit- ment)	0/1	0/1	0/1
	keyEncipherment	0/1	0/1	0/1
	dataEncipherment	0	0	0
	keyAgreement	0/1	0/1	1
	keyCertSign	1	1	0
	cRLSign	0	0	0
	encipherOnly	0	0	0
	decipherOnly	0	0	0
	ExtendedKeyUsage	-	-	x / c id-ce-extKeyUsage
	keyPurposeId	-	-	x id-kp-serverAuth
Extensions	CertificatePolicies	(x) / nc	(x) / nc	(x) / nc
	policyInformation	x	x	x
	certPolicyId	x (OID of the policy)	x (OID of the policy)	x (OID of the policy)
	policyQualifierInfo	(x)	(x)	(x)
	policyQualifierId	x id-qt-cps	x id-qt-cps	x id-qt-cps
	qualifier	x CPSuri	x CPSuri	x CPSuri
	cPSuri	x (CPS URI)	x (CPS URI)	x (CPS URI)
	userNotice	-	-	-
	policyInformation	(x)	(x)	(x)
	:	:	:	:
	policyInformation	(x)	(x)	(x)

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.5 (continued)**

ISO 15118-20 certificate profiles		Charge point operator		
		CSO Sub-CA 1 Sub	CSO Sub-CA 2 Sub	SECC Cert Leaf
BasicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints
cA	TRUE	TRUE	TRUE	FALSE
pathLenConstraint	1	0	-	-
CRLDistributionPoints (CRL)	-	-	-	-
AuthorityInfoAccess	x / nc id-pe-authorityInfoAccess	x / nc id-pe-authorityInfoAccess	x / nc id-pe-authorityInfoAccess	x / nc id-pe-authorityInfoAccess
accessDescription (OCSP)	x	x	x	x
accessMethod	x id-ad-ocsp	x id-ad-ocsp	x id-ad-ocsp	x id-ad-ocsp
accessLocation	x (URI of the OCSP responder)	x (URI of the OCSP responder)	x (URI of the OCSP responder)	x (URI of the OCSP responder)
generalName	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]
accessDescription	-	-	-	-
SubjectInfoAccess	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	-
accessDescription (CrossCertIndication)	x	x	-	-
accessMethod	x id-crossCertIndication (see [V2G20-2604])	x id-crossCertIndication (see [V2G20-2604])	x id-crossCertIndication (see [V2G20-2604])	-
accessLocation	x	x	-	-
generalName	x otherName [0]	x otherName [0]	-	-
type-id	x id-utf8String (see [V2G20-3077])	x id-utf8String (see [V2G20-3077])	-	-
value	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	-	-
accessDescription	-	-	-	-

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.5 (continued)

ISO 15118-20 certificate profiles		Charge point operator		SECC Cert Leaf
		CSO Sub-CA 1 Sub	CSO Sub-CA 2 Sub	
SignatureAl-gorithm	AlgorithmIdentifier	x	x	x
	algorithm	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512
	parameters	-	-	-
Signature Value		(Octet-String)	(Octet-String)	(Octet-String)

Delete NOTE 1 and NOTE 3 below Table B.5 and renumber NOTE 2.

Clause B.4.2

Replace Table B.6 with this table:

Table B.6 — Charge point operator certificates based on curves as defined by [V2G20-2319]

ISO 15118-20 certificate profiles		Charge point operator		
		CSO Sub-CA 1 Sub	CSO Sub-CA 2 Sub	SECC Cert Leaf
Signature	Version	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)
	SerialNumber	x	x	x
	AlgorithmIdentifier	x	x	x
Issuer	algorithm	x id-Ed448	x id-Ed448	x id-Ed448
	parameters	-	-	-
	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)
Validity	Common Name (CN)	x	x	x
	Domain Component (DC)	(x)	(x)	(x)
Validity	Validity	x [up to CSO]	x [up to CSO]	x [up to CSO]

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.6 (continued)

ISO 15118-20 certificate profiles		Charge point operator		SECC Cert Leaf
		CSO Sub-CA 1 Sub	CSO Sub-CA 2 Sub	
Subject	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	x (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)
	Common Name (CN)	x	x	x SECCID (see [V2G20-2583])
	Domain Component (DC)	(x)	(x)	(x) & "CSO"
Subject-PublicKey-Info	AlgorithmIdentifier	x	x	x
	algorithm	x id-Ed448	x id-Ed448	x id-Ed448
	parameters	-	-	-
	SubjectPublicKey	x (BIT STRING)	x (BIT STRING)	x (BIT STRING)
IssuerUniqueID		-	-	-
SubjectUniqueID		-	-	-
TbsCertificate	AuthorityKeyIdentifier	x / nc id-ce-authorityKey-Identifier	x / nc id-ce-authorityKey-Identifier	x / nc id-ce-authorityKey-Identifier
	keyIdentifier	x (see [V2G20-1851])	x (see [V2G20-1851])	x (see [V2G20-1851])
	authorityCertIssuer	-	-	-
	authorityCertSerialNumber	-	-	-
	SubjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier
	keyIdentifier	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])
	KeyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage
	digitalSignature	0/1	0/1	1
	nonRepudiation (contentCommitment)	0/1	0/1	0/1
	keyEncipherment	0/1	0/1	0/1
	dataEncipherment	0	0	0
	keyAgreement	0/1	0/1	0/1
	keyCertSign	1	1	0
	cRLSign	0	0	0
	encipherOnly	0	0	0

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.6 (continued)**

ISO 15118-20 certificate profiles		Charge point operator		SECC Cert Leaf
		CSO Sub-CA 1 Sub	CSO Sub-CA 2 Sub	
Extensions	decipherOnly	0	0	0
	ExtendedKeyUsage	-	-	x / c id-ce-extKeyUsage
	keyPurposeId	-	-	x id-kp-serverAuth
	CertificatePolicies	(x) / nc	(x) / nc	(x) / nc
	policyInformation	x	x	x
	certPolicyId	x (OID of the policy)	x (OID of the policy)	x (OID of the policy)
	policyQualifierInfo	(x)	(x)	(x)
	policyQualifierId	x id-qt-cps	x id-qt-cps	x id-qt-cps
	qualifier	x CPSuri	x CPSuri	x CPSuri
	cPSuri	x (CPS URI)	x (CPS URI)	x (CPS URI)
	userNotice	-	-	-
	policyInformation	(x)	(x)	(x)
	:	:	:	:
	:	:	:	:
	policyInformation	(x)	(x)	(x)
	BasicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints
	cA	TRUE	TRUE	FALSE
	pathLenConstraint	1	0	-
	CRLDistribution-Points (CRL)	-	-	-
	AuthorityInfoAccess	x / nc id-pe-authorityInfoAccess	x / nc id-pe-authorityInfoAccess	x / nc id-pe-authorityInfoAccess
	accessDescription (OCSP)	x	x	x
	accessMethod	x id-ad-ocsp	x id-ad-ocsp	x id-ad-ocsp
	accessLocation	x (URI of the OCSP responder)	x (URI of the OCSP responder)	x (URI of the OCSP responder)
	generalName	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]
	accessDescription	-	-	-

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.6 (continued)

ISO 15118-20 certificate profiles		Charge point operator		SECC Cert Leaf
		CSO Sub-CA 1 Sub	CSO Sub-CA 2 Sub	
	SubjectInfoAccess	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	-
	accessDescription (CrossCertIndication)	x	x	-
	accessMethod	x id-crossCertIndication (see [V2G20-2604])	x id-crossCertIndication (see [V2G20-2604])	-
	accessLocation	x	x	-
	generalName	x otherName [0]	x otherName [0]	-
	type-id	x id-utf8String (see [V2G20-3077])	x id-utf8String (see [V2G20-3077])	-
	value	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	-
Signature-Algorithm	AlgorithmIdentifier	x	x	x
	algorithm	x id-Ed448	x id-Ed448	x id-Ed448
	parameters	-	-	-
Signature Value		(Raw BIT STRING)	(Raw BIT STRING)	(Raw BIT STRING)

Delete NOTE below Table B.6

Clause B.4.3

Replace the first paragraph with:

As mentioned in Table B.5 and Table B.6, it is optional to include the ‘certificatePolicies’ extension in any of the charge point operator certificates. If the ‘certificatePolicies’ extension is included, it can be marked as non-critical so that, if allowed by the local policy, the relying party can ignore this extension if it cannot process it. This is done to improve the interoperability.

Add the following new requirements and text below requirement [V2G20-2584]:

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

- [V2G20-3049]** Subject field of the SECC Leaf Certificate shall contain Domain Component ending with "CSO".
- [V2G20-3050]** The CA, at it's discretion, may include any other necessary information in the Domain Component RDN of the Subject field of the SECC Leaf Certificate without violating **[V2G20-3049]**.

As mentioned in Table B.5 and Table B.6, 'AuthorityInfoAccess' extension in any of the certificates in the SECC certificate chain is non-critical. As the EVCC receives the OCSP response for all the certificates in SECC certificate chain during the TLS handshake, normally the EVCC does not need to process 'AuthorityInfoAccess' extension in any of the certificates in the SECC certificate chain.

As such, the EVCC is neither required to nor prohibited from processing 'AuthorityInfoAccess' extension in any of the certificates in the SECC certificate chain. It is left upto the local policy of the EVCC whether 'AuthorityInfoAccess' extension is processed or not.

Clause B.5.1

Replace Table B.7 with this table:

Table B.7 — Certificate installation (provisioning) service certificates based on curves as defined by [V2G20-2674]

ISO 15118-20 certificate profiles		Certificate provisioning service		
		CPS Sub-CA 1 Sub	CPS Sub-CA 2 Sub	CPS Leaf Cert Leaf
	Version	2 (“2” indicates X.509v3)	2 (“2” indicates X.509v3)	2 (“2” indicates X.509v3)
	SerialNumber	x	x	x
Signature	AlgorithmIdentifier	x	x	x
	algorithm	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512
	parameters	-	-	-
Issuer	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)
	Common Name (CN)	x	x	x
	Domain Component (DC)	(x)	(x)	(x)
Validity	Validity	x [up to CPS]	x [up to CPS]	x [up to CPS]

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.7 (continued)

ISO 15118-20 certificate profiles		Certificate provisioning service		
		CPS Sub-CA 1 Sub	CPS Sub-CA 2 Sub	CPS Leaf Cert Leaf
Subject	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	x (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)
	Common Name (CN)	x	x	x
	Domain Component (DC)	(x)	(x)	(x) & "CPS"
Subject-PublicKey-Info	AlgorithmIdentifier	x	x	x
	algorithm	x id-ecPublicKey	x id-ecPublicKey	x id-ecPublicKey
	parameters (ECParameters)	x	x	x
	namedCurve	x secp521r1	x secp521r1	x secp521r1
	SubjectPublicKey	x (BIT STRING)	x (BIT STRING)	x (BIT STRING)
IssuerUniqueID		-	-	-
SubjectUniqueID		-	-	-
KeyUsage	AuthorityKeyIdentifier	x / nc id-ce-authorityKey-Identifier	x / nc id-ce-authorityKey-Identifier	x / nc id-ce-authorityKey-Identifier
	keyIdentifier	x (see [V2G20-1851])	x (see [V2G20-1851])	x (see [V2G20-1851])
	authorityCertIssuer	-	-	-
	authorityCertSerialNumber	-	-	-
	SubjectKeyIdentifier	x / nc id-ce-subjectKey-Identifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier
	keyIdentifier	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])
	KeyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage
	digitalSignature	0/1	0/1	1
	nonRepudiation (contentCommitment)	0/1	0/1	0/1
	keyEncipherment	0/1	0/1	0/1
	dataEncipherment	0	0	0
	keyAgreement	0/1	0/1	0
	keyCertSign	1	1	0
	cRLSign	0	0	0
	encipherOnly	0	0	0
	decipherOnly	0	0	0

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.7 (continued)

ISO 15118-20 certificate profiles		Certificate provisioning service		
		CPS Sub-CA 1 Sub	CPS Sub-CA 2 Sub	CPS Leaf Cert Leaf
TbsCertifi- cate	ExtendedKeyUsage	-	-	-
	CertificatePolicies	(x) / nc	(x) / nc	(x) / nc
	policyInformation	x	x	x
	certPolicyId	x (OID of the policy)	x (OID of the policy)	x (OID of the policy)
	policyQualifierInfo	(x)	(x)	(x)
	policyQualifierId	x id-qt-cps	x id-qt-cps	x id-qt-cps
	qualifier	x CPSuri	x CPSuri	x CPSuri
	cPSuri	x (CPS URI)	x (CPS URI)	x (CPS URI)
	userNotice	-	-	-
	policyInformation	(x)	(x)	(x)
	:	:	:	:
	:	:	:	:
	policyInformation	(x)	(x)	(x)
	BasicConstraints	x / c id-ce-basicCon- straints	x / c id-ce-basicCon- straints	x / c id-ce-basicCon- straints
Extensions	cA	TRUE	TRUE	FALSE
	pathLenConstraint	1	0	-
	CRLDistribution- Points	(x) / nc id-ce-cRLDistribu- tionPoints	(x) / nc id-ce-cRLDistribu- tionPoints	(x) / nc id-ce-cRLDistribu- tionPoints
	distributionPoint	x	x	x
	distributionPoint- Name	(x) (see [V2G20-3038] and B.2.3.2.1)	(x) (see [V2G20-3038] and B.2.3.2.1)	(x) (see [V2G20-3038] and B.2.3.2.1)
	fullName	x (in GeneralNames format)	x (in GeneralNames format)	x (in GeneralNames format)
	generalName	x uniformResourceI- dentifier [6]	x uniformResourceI- dentifier [6]	x uniformResourceI- dentifier [6]
	nameRela- tiveToCRLIssuer	-	-	-
	reasons	-	-	-
	cRLIssuer	(x) (see B.2.3.2.1)	(x) (see B.2.3.2.1)	(x) (see B.2.3.2.1)
	distributionPoint	-	-	-
	AuthorityInfoAc- cess	(x) / nc id-pe-authorityIn- foAccess	(x) / nc id-pe-authorityIn- foAccess	(x) / nc id-pe-authorityIn- foAccess

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.7 (continued)

ISO 15118-20 certificate profiles		Certificate provisioning service		
		CPS Sub-CA 1 Sub	CPS Sub-CA 2 Sub	CPS Leaf Cert Leaf
Signature-Algorithm	accessDescription (OCSP)	x	x	x
	accessMethod	x id-ad-ocsp	x id-ad-ocsp	x id-ad-ocsp
	accessLocation	x (URI of the OCSP responder)	x (URI of the OCSP responder)	x (URI of the OCSP responder)
	generalName	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]
	accessDescription	-	-	-
	SubjectInfoAccess	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	-
	accessDescription (CrossCertIndication)	x	x	-
	accessMethod	x id-crossCertIndication (see [V2G20-2604])	x id-crossCertIndication (see [V2G20-2604])	-
	accessLocation	x	x	-
	generalName	x otherName [0]	x otherName [0]	-
	type-id	x id-utf8String (see [V2G20-3077])	x id-utf8String (see [V2G20-3077])	-
	value	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	-
	accessDescription	-	-	-
Signature-Algorithm	AlgorithmIdentifier	x	x	x
	algorithm	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512
	parameters	-	-	-
Signature Value		(Octet-String)	(Octet-String)	(Octet-String)

Delete NOTE 1 below Table B.7 and renumber NOTE 2.

Clause B.5.2

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Replace Table B.8 with this table:

Table B.8 — Certificate installation (provisioning) service certificates based on curves as defined by [V2G20-2319]

ISO 15118-20 certificate profiles		Certificate provisioning service		
		CPS Sub-CA 1 Sub	CPS Sub-CA 2 Sub	CPS Leaf Cert Leaf
Version		2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)
SerialNumber		(Positive integer)	(Positive integer)	(Positive integer)
Signature	AlgorithmIdentifier	x	x	x
	algorithm	x id-Ed448	x id-Ed448	x id-Ed448
	parameters	-	-	-
Issuer	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)
	Common Name (CN)	x	x	x
	Domain Component (DC)	(x)	(x)	(x)
Validity	Validity	x [up to CPS]	x [up to CPS]	x [up to CPS]
Subject	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	x (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)
	Common Name (CN)	x	x	x
	Domain Component (DC)	(x)	(x)	(x) & "CPS"
Subject-PublicKey-Info	AlgorithmIdentifier	x	x	x
	algorithm	x id-Ed448	x id-Ed448	x id-Ed448
	parameters	-	-	-
	SubjectPublicKey	x (BIT STRING)	x (BIT STRING)	x (BIT STRING)
IssuerUniqueID		-	-	-
SubjectUniqueID		-	-	-
	AuthorityKeyIdentifier	x / nc id-ce-authorityKey-Identifier	x / nc id-ce-authorityKey-Identifier	x / nc id-ce-authorityKey-Identifier
	keyIdentifier	x (see [V2G20-1851])	x (see [V2G20-1851])	x (see [V2G20-1851])
	authorityCertIssuer	-	-	-

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.8 (continued)

ISO 15118-20 certificate profiles		Certificate provisioning service		
		CPS Sub-CA 1 Sub	CPS Sub-CA 2 Sub	CPS Leaf Cert Leaf
TbsCertificate	authorityCertSerialNumber	-	-	-
	SubjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier
	keyIdentifier	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])
	KeyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage
	digitalSignature	0/1	0/1	1
	nonRepudiation (contentCommitment)	0/1	0/1	0/1
	keyEncipherment	0/1	0/1	0/1
	dataEncipherment	0	0	0
	keyAgreement	0/1	0/1	0
	keyCertSign	1	1	0
	cRLSign	0	0	0
	encipherOnly	0	0	0
	decipherOnly	0	0	0
	ExtendedKeyUsage	-	-	-
	CertificatePolicies	(x) / nc	(x) / nc	(x) / nc
	policyInformation	x	x	x
	certPolicyId	x (OID of the policy)	x (OID of the policy)	x (OID of the policy)
	policyQualifierInfo	(x)	(x)	(x)
	policyQualifierId	x id-qt-cps	x id-qt-cps	x id-qt-cps
	qualifier	x CPSuri	x CPSuri	x CPSuri
	cPSuri	x (CPS URI)	x (CPS URI)	x (CPS URI)
	userNotice	-	-	-
	policyInformation	(x)	(x)	(x)
	:	:	:	:
	:	:	:	:
	policyInformation	(x)	(x)	(x)
	BasicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints
	cA	TRUE	TRUE	FALSE
	pathLenConstraint	1	0	-
	CRLDistributionPoints	(x) / nc id-ce-cRLDistributionPoints	(x) / nc id-ce-cRLDistributionPoints	(x) / nc id-ce-cRLDistributionPoints
Extensions				

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.8 (continued)

ISO 15118-20 certificate profiles		Certificate provisioning service		
		CPS Sub-CA 1 Sub	CPS Sub-CA 2 Sub	CPS Leaf Cert Leaf
	distributionPoint	x	x	x
	distributionPoint-Name	(x) (see [V2G20-3038] and B.2.3.2.1)	(x) (see [V2G20-3038] and B.2.3.2.1)	(x) (see [V2G20-3038] and B.2.3.2.1)
	fullName	x (in GeneralNames format)	x (in GeneralNames format)	x (in GeneralNames format)
	generalName	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]
	nameRelativeToCRLIssuer	-	-	-
	reasons	-	-	-
	cRLIssuer	(x) (see B.2.3.2.1)	(x) (see B.2.3.2.1)	(x) (see B.2.3.2.1)
	distributionPoint	-	-	-
	AuthorityInfoAccess	(x) / nc id-pe-authorityInfoAccess	(x) / nc id-pe-authorityInfoAccess	(x) / nc id-pe-authorityInfoAccess
	accessDescription (OCSP)	x	x	x
	accessMethod	x id-ad-ocsp	x id-ad-ocsp	x id-ad-ocsp
	accessLocation	x (URI of the OCSP responder)	x (URI of the OCSP responder)	x (URI of the OCSP responder)
	generalName	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]
	accessDescription	-	-	-
	SubjectInfoAccess	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	-
	accessDescription (CrossCertIndication)	x	x	-
	accessMethod	x id-crossCertIndication (see [V2G20-2604])	x id-crossCertIndication (see [V2G20-2604])	-
	accessLocation	x	x	-
	generalName	x otherName [0]	x otherName [0]	-

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.8 (continued)

ISO 15118-20 certificate profiles		Certificate provisioning service		
		CPS Sub-CA 1 Sub	CPS Sub-CA 2 Sub	CPS Leaf Cert Leaf
	type-id	x id-utf8String (see [V2G20-3077])	x id-utf8String (see [V2G20-3077])	-
	value	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	-
	accessDescription	-	-	-
Signature-Algorithm	AlgorithmIdentifier	x	x	x
	algorithm	x id-Ed448	x id-Ed448	x id-Ed448
	parameters	-	-	-
Signature Value		(Raw BIT STRING)	(Raw BIT STRING)	(Raw BIT STRING)

Clause B.5.3

Replace entire text in this clause with:

As mentioned in Table B.7 and Table B.8, it is optional to include the ‘certificatePolicies’ extension in any of the charge point operator certificates. If the ‘certificatePolicies’ extension is included, it should be marked as non-critical so that, if allowed by the local policy, the relying party can ignore this extension if it cannot process it. This is done to improve the interoperability.

- [V2G20-3051] Subject field of the CPS Leaf Certificate shall contain Domain Component ending with “CPS”.
- [V2G20-3052] The CA, at its discretion, may include any other necessary information in the Domain Component RDN of the Subject field of the CPS Leaf Certificate without violating [V2G20-3051].
- [V2G20-2585] If the CPS Sub CA1 Certificate or CPS Sub CA2 Certificate or CPS Leaf Certificate contains both ‘CRLDistributionPoints’ and ‘AuthorityInfoAccess’ extensions, the relying party may process just one or both or none as per the local policy of the relying party.

NOTE 1 Table B.7 and Table B.8 specify that both ‘CRLDistributionPoints’ and ‘AuthorityInfoAccess’ extensions are optional and non-critical to indicate that either of them can be included but that it is not mandatory for the receiver of these certificates to process these extensions. This requirement clarifies that if the issuer desires to include both of these, it is up to the relying party to decide which one to process, if any.

- [V2G20-2586] The EVCC is not mandated to process CRLDistributionPoints extension and/or ‘AuthorityInfoAccess’ extension if either or both are present in CPS Sub CA1 certificate or CPS Sub CA2 certificate or CPS leaf certificate.

NOTE 2 EVCC is not required to process ‘CRLDistributionPoints’ extension. The EVCC, however, is allowed to process ‘CRLDistributionPoints’ extension if its local policy requires it to do so. This document does not define any methodology (message) for the SECC and/or SA to provide the CRL data for the CPS certificate chain to the EVCC. Hence, EVCC should only process ‘CRLDistributionPoints’ extension in any of the certificate provisioning service certificates if and only if the EVCC has independent capability to reach the CRL distribution point, receive the CRL data and process it.

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

NOTE 3 EVCC is not required to process 'AuthorityInfoAccess' extension. The EVCC, however, is allowed to process 'AuthorityInfoAccess' extension if its local policy requires it to do so. This document does not define any methodology (message) for the SECC and/or SA to provide the OCSP response for the CPS certificate chain to the EVCC. Hence, EVCC should only process 'AuthorityInfoAccess' extension in any of the certificate provisioning service certificates if and only if the EVCC has independent capability to reach the OCSP responder, receive the OCSP response and process it.

Clause B.6.1

Replace Table B.9 with this table:

Table B.9 — e-Mobility service provider certificates based on curves as defined by [V2G20-2674]

ISO 15118-20 certificate profiles		eMSP Root CA Root	eMSP Sub-CA 1 Sub	eMSP Sub-CA 2 Sub/Leaf	e-Mobility service provider Contract Cert Leaf
Version		2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)
SerialNumber		x	x	x	x
Signature	AlgorithmIdentifier	x	x	x	x
	algorithm	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512
	parameters	-	-	-	-
Issuer	Country (C)	(x) (ISO 3166-1 alpha-2 code)			
	Organization (O)	x	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)	(x)
	Common Name (CN)	x	x	x	x
	Domain Component (DC)	(x)	(x)	(x)	(x)
Validity	Validity	x [up to eMSP]	x [up to eMSP]	x [up to eMSP]	x [up to eMSP]
Subject	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	x (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)	(x)
	Common Name (CN)	x	x	x	x EMAID (see [V2G20-2588])
	Domain Component (DC)	(x)	(x)	(x)	(x)

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.9 (continued)

ISO 15118-20 certificate profiles		e-Mobility service provider			
		eMSP Root CA Root	eMSP Sub-CA 1 Sub	eMSP Sub-CA 2 Sub/Leaf	Contract Cert Leaf
Subject-PublicKey-Info	AlgorithmIdentifier	x	x	x	x
	algorithm	x id-ecPublic-Key	x id-ecPublic-Key	x id-ecPublic-Key	x id-ecPublicKey
	parameters (ECParameters)	x	x	x	x
	namedCurve	x secp521r1	x secp521r1	x secp521r1	x secp521r1
	SubjectPublicKey	x (BIT STRING)	x (BIT STRING)	x (BIT STRING)	x (BIT STRING)
IssuerUniqueID		-	-	-	-
SubjectUniqueID		-	-	-	-
	AuthorityKeyIdentifier	-	x / nc id-ce-authorityKey-Identifier	x / nc id-ce-authorityKey-Identifier	x / nc id-ce-authorityKeyIdentifier
	keyIdentifier	-	x (see [V2G20-1851])	x (see [V2G20-1851])	x (see [V2G20-1851])
	authorityCertIssuer	-	-	-	-
	authorityCertSerialNumber	-	-	-	-
	SubjectKeyIdentifier	x / nc id-ce-subjectKey-Identifier	x / nc id-ce-subjectKey-Identifier	x / nc id-ce-subjectKey-Identifier	x / nc id-ce-subjectKeyIdentifier
	keyIdentifier	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])
	KeyUsage	x / c id-ce-key-Usage	x / c id-ce-key-Usage	x / c id-ce-key-Usage	x / c id-ce-keyUsage
	digitalSignature	0/1	0/1	0/1	1
	nonRepudiation (contentCommitment)	0/1	0/1	0/1	0/1
	keyEncipherment	0/1	0/1	0/1	0/1
	dataEncipherment	0	0	0	0
	keyAgreement	0/1	0/1	0/1	0
	keyCertSign	1	1	1	0
	cRLSign	0	0	0	0
	encipherOnly	0	0	0	0

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.9 (continued)**

ISO 15118-20 certificate profiles		e-Mobility service provider			
		eMSP Root CA Root	eMSP Sub-CA 1 Sub	eMSP Sub-CA 2 Sub/Leaf	Contract Cert Leaf
TbsCertificate	decipherOnly	0	0	0	0
	ExtendedKey-Usage	-	-	-	-
	CertificatePolicies	-	(x) / nc	(x) / nc	(x) / nc
	policyInformation	-	x	x	x
	certPolicyId	-	x (OID of the policy)	x (OID of the policy)	x (OID of the policy)
	policyQualifier-Info	-	(x)	(x)	(x)
	policyQualifierId	-	x id-qt-cps	x id-qt-cps	x id-qt-cps
	qualifier	-	x CPSuri	x CPSuri	x CPSuri
	cPSuri	-	x (CPS URI)	x (CPS URI)	x (CPS URI)
	userNotice	-	-	-	-
	policyInformation	-	(x)	(x)	(x)
	:	-	:	:	:
	:	-	:	:	:
	policyInformation	-	(x)	(x)	(x)
	BasicConstraints	x / c id-ce-basic-Constraints	x / c id-ce-basic-Constraints	x / c id-ce-basic-Constraints	x / c id-ce-basicConstraints
	cA	TRUE	TRUE	TRUE	FALSE
	pathLenCon-straint	-	1	0	-
	CRLDistribution-Points (CRL)	-	(x) / nc id-ce-cRLD-istribution-Points	(x) / nc id-ce-cRLD-istribution-Points	(x) / nc id-ce-cRLDistributionPoints
	distributionPoint	-	x	x	x
	distributionPoint-Name	-	(x) (see [V2G20-3038] and B.2.3.2.1)	(x) (see [V2G20-3038] and B.2.3.2.1)	(x) (see [V2G20-3038] and B.2.3.2.1)
	fullName	-	x (in GeneralNames format)	x (in GeneralNames format)	x (in GeneralNames format)
	generalName	-	x uniformRe-sourceIdentifier [6]	x uniformRe-sourceIdentifier [6]	x uniformResourceIdentifier [6]
	nameRela-tiveToCRLIssuer	-	-	-	-

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.9 (continued)**

ISO 15118-20 certificate profiles		e-Mobility service provider			
		eMSP Root CA Root	eMSP Sub-CA 1 Sub	eMSP Sub-CA 2 Sub/Leaf	Contract Cert Leaf
Extensions	reasons	-	-	-	-
	cRLIssuer	-	(x) (see B.2.3.2.1)	(x) (see B.2.3.2.1)	(x) (see B.2.3.2.1)
	distributionPoint	-	-	-	-
	AuthorityInfoAccess	-	(x) / nc id-pe-authorityInfoAccess	(x) / nc id-pe-authorityInfoAccess	(x) / nc id-pe-authorityInfoAccess
	accessDescription (OCSP)	-	x	x	x
	accessMethod	-	x id-ad-ocsp	x id-ad-ocsp	x id-ad-ocsp
	accessLocation	-	x (URI of the OCSP responder)	x (URI of the OCSP responder)	x (URI of the OCSP responder)
	generalName	-	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]
	accessDescription	-	-	-	-
	SubjectInfoAccess	-	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	(x) / nc id-pe-subjectInfoAccess
	accessDescription (ContractMobilityOperatorName)	-	-	-	(x)
	accessMethod	-	-	-	x id-contractOperatorName (see [V2G20-1226])
	accessLocation	-	-	-	x
	generalName	-	-	-	x otherName [0]
	type-id	-	-	-	x id-utf8String (see [V2G20-3056])

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.9 (continued)

ISO 15118-20 certificate profiles		e-Mobility service provider			Contract Cert
		eMSP Root CA Root	eMSP Sub-CA 1 Sub	eMSP Sub-CA 2 Sub/Leaf	
	value	-	-	-	x (A user-friendly name of the eMSP for direct display in the vehicle that issued the contract. Maximum allowed length is 255 bytes)
	accessDescription (ContractTariff-Name)	-	-	-	(x)
	accessMethod	-	-	-	x id-contractTariffName (see [V2G20-1226])
	accessLocation	-	-	-	x
	generalName	-	-	-	x otherName [0]
	type-id	-	-	-	x id-utf8String (see [V2G20-3056])
	value	-	-	-	x (A user-friendly name of the Tariff for direct display in the vehicle. Maximum allowed length is 255 bytes)
	accessDescription (ContractDynamicInformationUrl)	-	-	-	(x)
	accessMethod	-	-	-	x id-contractDynamicInformationUrl (see [V2G20-1226])
	accessLocation	-	-	-	x (A URL to a distribution point of current (daily) additional information to the contract Syntax: An alphanumeric string with a maximum length of 255 characters)
	generalName	-	-	-	x uniformResourceIdentifier [6]
accessDescription		-	-	-	-
accessDescription (CrossCertIndication)		-	x	x	-

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.9 (continued)

ISO 15118-20 certificate profiles		e-Mobility service provider			Contract Cert
		eMSP Root CA Root	eMSP Sub-CA 1 Sub	eMSP Sub-CA 2 Sub/Leaf	
	accessMethod	-	x id-cross-CertIndication (see [V2G20-2604])	x id-cross-CertIndication (see [V2G20-2604])	-
	accessLocation	-	x	x	-
	generalName	-	x otherName [0]	x otherName [0]	-
	type-id	-	x id-utf-8String (see [V2G20-3077])	x id-utf-8String (see [V2G20-3077])	-
	value	-	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	-
	accessDescription	-	-	-	-
Signature-Algorithm	AlgorithmIdentifier	x	x	x	x
	algorithm	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512
	parameters	-	-	-	-
Signature Value		(Octet-String)	(Octet-String)	(Octet-String)	(Octet-String)

Delete NOTE 1 below Table B.9 and renumber NOTE 2 and NOTE 3.

Clause B.6.2

Replace Table B.10 with this table:

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.10 — e-Mobility service provider certificates based on curves as defined by [V2G20-2319]

ISO 15118-20 certificate profiles		e-Mobility service provider			
		eMSP Root CA Root	eMSP Sub-CA 1 Sub	eMSP Sub-CA 2 Sub/Leaf	Contract Cert Leaf
	Version	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)
	SerialNumber	x	x	x	x
Signature	AlgorithmIdentifier	x	x	x	x
	algorithm	x id-Ed448	x id-Ed448	x id-Ed448	x id-Ed448
	parameters	-	-	-	-
Issuer	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)	(x)
	Common Name (CN)	x	x	x	x
	Domain Component (DC)	(x)	(x)	(x)	(x)
Validity	Validity	x [up to eMSP]	x [up to eMSP]	x [up to eMSP]	x [up to eMSP]
Subject	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	x (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)	(x)
	Common Name (CN)	x	x	x	x EMAID (see [V2G20-2588])
	Domain Component (DC)	(x)	(x)	(x)	(x)
Subject-PublicKey-Info	AlgorithmIdentifier	x	x	x	x
	algorithm	x id-Ed448	x id-Ed448	x id-Ed448	x id-Ed448
	parameters	-	-	-	-
	SubjectPublicKey	x (BIT STRING)	x (BIT STRING)	x (BIT STRING)	x (BIT STRING)
IssuerUniqueID		-	-	-	-
SubjectUniqueID		-	-	-	-

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.10 (continued)

ISO 15118-20 certificate profiles		e-Mobility service provider			Contract Cert
		eMSP Root CA Root	eMSP Sub-CA 1 Sub	eMSP Sub-CA 2 Sub/Leaf	
AuthorityKeyIdentifier	-	x / nc id-ce-authorityKeyIdentifier	x / nc id-ce-authorityKeyIdentifier	x / nc id-ce-authorityKeyIdentifier	x / nc id-ce-authorityKeyIdentifier
keyIdentifier	-	x (see [V2G20-1851])	x (see [V2G20-1851])	x (see [V2G20-1851])	x (see [V2G20-1851])
authorityCertIssuer	-	-	-	-	-
authorityCertSerialNumber	-	-	-	-	-
SubjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier
keyIdentifier	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])
KeyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage
digitalSignature	0/1	0/1	0/1	0/1	1
nonRepudiation (contentCommitment)	0/1	0/1	0/1	0/1	0/1
keyEncipherment	0/1	0/1	0/1	0/1	0/1
dataEncipherment	0	0	0	0	0
keyAgreement	0/1	0/1	0/1	0/1	0
keyCertSign	1	1	1	1	0
cRLSign	0	0	0	0	0
encipherOnly	0	0	0	0	0
decipherOnly	0	0	0	0	0
ExtendedKeyUsage	-	-	-	-	-
CertificatePolicies	-	(x) / nc	(x) / nc	(x) / nc	(x) / nc
policyInformation	-	x	x	x	x
certPolicyId	-	x (OID of the policy)			
policyQualifierInfo	-	(x)	(x)	(x)	(x)
policyQualifierId	-	x id-qt-cps	x id-qt-cps	x id-qt-cps	x id-qt-cps
qualifier	-	x CPSuri	x CPSuri	x CPSuri	x CPSuri

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.10 (continued)**

ISO 15118-20 certificate profiles		e-Mobility service provider			
		eMSP Root CA Root	eMSP Sub-CA 1 Sub	eMSP Sub-CA 2 Sub/Leaf	Contract Cert Leaf
TbsCertificate	cPSuri	-	x (CPS URI)	x (CPS URI)	x (CPS URI)
	userNotice	-	-	-	-
	policyInformation	-	(x)	(x)	(x)
	:	-	:	:	:
	:	-	:	:	:
	policyInformation	-	(x)	(x)	(x)
	BasicConstraints	x / c id-ce-basic- Constraints	x / c id-ce-basic- Constraints	x / c id-ce-basic- Constraints	x / c id-ce-basicConstraints
	cA	TRUE	TRUE	TRUE	FALSE
	pathLenCon- straint	-	1	0	-
	CRLDistribution- Points (CRL)	-	(x) / nc id-ce-cRLD- istribution- Points	(x) / nc id-ce-cRLD- istribution- Points	(x) / nc id-ce-cRLDDistributionPoints
	distributionPoint	-	x	x	x
	distributionPoint- Name	-	(x) (see [V2G20- 3038] and B.2.3.2.1)	(x) (see [V2G20- 3038] and B.2.3.2.1)	(x) (see [V2G20-3038] and B.2.3.2.1)
	fullName	-	x (in Gener- alNames format)	x (in Gener- alNames format)	x (in GeneralNames format)
	generalName	-	x uniformRe- sourceIden- tifier [6]	x uniformRe- sourceIden- tifier [6]	x uniformResourceIdentifier [6]
	nameRela- tiveToCRLIssuer	-	-	-	-
	reasons	-	-	-	-
	cRLIssuer	-	(x) (see B.2.3.2.1)	(x) (see B.2.3.2.1)	(x) (see B.2.3.2.1)
	distributionPoint	-	-	-	-
	AuthorityInfoAc- cess	-	(x) / nc id-pe-au- thorityIn- foAccess	(x) / nc id-pe-au- thorityIn- foAccess	(x) / nc id-pe-authorityInfoAccess
	accessDescription (OCSP)	-	x	x	x
	accessMethod	-	x id-ad-ocsp	x id-ad-ocsp	x id-ad-ocsp

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.10 (continued)

ISO 15118-20 certificate profiles		e-Mobility service provider			
		eMSP Root CA Root	eMSP Sub-CA 1 Sub	eMSP Sub-CA 2 Sub/Leaf	Contract Cert Leaf
Extensions	accessLocation	-	x (URI of the OCSP responder)	x (URI of the OCSP responder)	x (URI of the OCSP responder)
	generalName	-	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]
	accessDescription	-	-	-	-
	SubjectInfoAccess	-	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	(x) / nc id-pe-subjectInfoAccess
	accessDescription (ContractMobilityOperatorName)	-	-	-	(x)
	accessMethod	-	-	-	x id-contractOperatorName (see [V2G20-1226])
	accessLocation	-	-	-	x
	generalName	-	-	-	x otherName [0]
	type-id	-	-	-	x id-utf8String (see [V2G20-3056])
	value	-	-	-	x (A user-friendly name of the eMSP for direct display in the vehicle that issued the contract. Maximum allowed length is 255 bytes)
	accessDescription (ContractTariff-Name)	-	-	-	(x)
	accessMethod	-	-	-	x id-contractTariffName (see [V2G20-1226])
	accessLocation	-	-	-	x
	generalName	-	-	-	x otherName [0]

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.10 (continued)

ISO 15118-20 certificate profiles		e-Mobility service provider			
		eMSP Root CA Root	eMSP Sub-CA 1 Sub	eMSP Sub-CA 2 Sub/Leaf	Contract Cert Leaf
	type-id	-	-	-	x id-utf8String (see [V2G20-3056])
	value	-	-	-	x (A user-friendly name of the Tariff for direct display in the vehicle. Maximum allowed length is 255 bytes)
	accessDescription (ContractDynamicInformationUrl)	-	-	-	(x)
	accessMethod	-	-	-	x id-contractDynamicInformationUrl (see [V2G20-1226])
	accessLocation	-	-	-	x (A URL to a distribution point of current (daily) additional information to the contract. Syntax: An alphanumeric string with a maximum length of 255 characters)
	generalName	-	-	-	x uniformResourceIdentifier [6]
	accessDescription (CrossCertIndication)	-	x	x	-
	accessMethod	-	x id-cross-CertIndication (see [V2G20-2604])	x id-cross-CertIndication (see [V2G20-2604])	-
	accessLocation	-	x	x	-
	generalName	-	x otherName [0]	x otherName [0]	-
	type-id	-	x id-utf-8String (see [V2G20-3077])	x id-utf-8String (see [V2G20-3077])	-

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.10 (continued)

ISO 15118-20 certificate profiles			eMSP Root CA Root	eMSP Sub-CA 1 Sub	eMSP Sub-CA 2 Sub/Leaf	e-Mobility service provider	Contract Cert Leaf
		value	-	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)		
		accessDescription		-	-	-	-
Signature-Algorithm	AlgorithmIdentifier		x	x	x	x	
	algorithm		x id-Ed448	x id-Ed448	x id-Ed448	x id-Ed448	
	parameters		-	-	-	-	
Signature Value			(Raw BIT STRING)	(Raw BIT STRING)	(Raw BIT STRING)	(Raw BIT STRING)	(Raw BIT STRING)

Clause B.6.3

Replace entire text in this clause with:

eMSP Sub-CA 2 has two purposes:

- It certifies contract certificates
- AND
- It signs tariff information destined for the owners of those contract certificates.

The ID of the provisioning certificate (PCID) is used by the eMSP to identify the contract that belongs to this EV. This is possible because the customer has given the PCID (CN and O, see L.4 and its subclauses for details) to the eMSP when creating the contract. For this purpose, PCID is supposed to be a short string that is unique to the OEM that created the provisioning certificate and to the vehicle which is requesting the contract certificate(s). Furthermore, it is contained in the provisioning certificate.

As mentioned in Table B.9 and Table B.10, it is optional to include the ‘certificatePolicies’ extension in any of the e-Mobility service provider certificates. If the ‘certificatePolicies’ extension is included, it can be marked as non-critical so that, if allowed by the local policy, the relying party can ignore this extension if it cannot process it. This is done to improve the interoperability.

It should be noted that the EVCC does not validate the contract certificate or any other certificates included in that chain. Usually, the SECC also does not validate the contract certificate or any other certificates included in that chain. Usually, the EVCC provides the contract certificate chain to the eMSP during AuthorizationReq. Customarily, it is up to the eMSP to validate the contract certificate chain and ensure that it meets the requirements. In rare instances, the SECC itself may validate the contract certificate chain for authorization purposes.

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

[V2G20-2588] EMAID shall be created per C.1.

[V2G20-2589] EMAID shall be contained in the subject field of the contract certificate as follows:

- The EMAID itself (see [V2G20-2588]) shall be the value of the Common Name (CN) of the Distinguished Name (DN).
- The name of the eMSP shall be encoded in the field Organization (O) using a unique identifier chosen by the eMSP, to identify this eMSP.
- The X.500 distinguished name in the subject field shall not contain any further values.

[V2G20-2590] eMSP Sub CA1 Certificate, eMSP Sub CA2 Certificate and Contract Certificate shall contain either 'CRLDistributionPoints' extension or 'AuthorityInfoAccess' extension or both.

NOTE 1 Table B.9 and Table B.10 specify that both 'CRLDistributionPoints' and 'AuthorityInfoAccess' extensions are optional to indicate that either one of them can be included. [V2G20-2590] clarifies that including at least one of them is mandatory while including both of them is not mandatory.

NOTE 2 [V2G20-2590] does not specify which one of these extensions can be included. It is left up to the eMSP to decide which certificate revocation method works best for it. In some cases CRLs will work better as they allow the relying party to download the entire CRL once and have it available for local checking of revocation status of the next contract certificate without a need for a live connection to the CRL server while in other cases OCSP will provide better results as it provides current revocation status and requires less storage and searching on part of the relying party.

[V2G20-2591] If eMSP Sub CA1 Certificate or eMSP Sub CA2 Certificate or Contract Certificate contains both 'CRLDistributionPoints' and 'AuthorityInfoAccess' extensions, the relying party may process just one or both as per the local policy of the relying party. However, the relying party shall process at least one of these extensions.

NOTE 3 Table B.9 and Table B.10 specify that both 'CRLDistributionPoints' and 'AuthorityInfoAccess' extensions are optional and [V2G20-2590] specifies that it is mandatory to include at least one of them. [V2G20-2591] clarifies that if the issuer desires to include both, it is up to the relying party to decide which one to process. [V2G20-2591] also ensures that the relying party will process at least one.

[V2G20-3053] If eMSP Sub CA1 Certificate or eMSP Sub CA2 Certificate or Contract Certificate contains only one of 'CRLDistributionPoints' and 'AuthorityInfoAccess' extensions, the relying party shall process the extension that is present.

NOTE 4 Table B.9 and Table B.10 specify that both 'CRLDistributionPoints' and 'AuthorityInfoAccess' extensions are optional and [V2G20-2590] specifies that it is mandatory to include at least one of them. [V2G20-2591] ensures that, if only one of them is included, the relying party will process that one.

[V2G20-1225] The Contract Certificate extensions in Table B.9 and Table B.10 shall use the definition of 'SubjectInfoAccess' as defined in IETF RFC 5280, 4.2.2.2, so that the issuer of a Contract Certificate can provide the vehicle with additional information and services. As mentioned in IETF RFC 5280, the field 'accessMethod' indicates the type of information and the field 'accessLocation' indicates either the information itself or a storage location for the information.

NOTE 5 IETF RFC 5280 has been updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399. These updates are considered to be included in this document.

[V2G20-1226] If the issuer of the certificate wishes to provide eMSP name in the contract certificate, it shall describe the information with one (1) additional access method for 'accessMethod'. Here are the definitions in ASN.1 notation:

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

```

ISO15118-Extensions { iso(1) standard(0) 15118 part20(20) extensions(0) }
DEFINITIONS :=
BEGIN

id-15118-20-ad          OBJECT IDENTIFIER := { iso(1) standard(0) 15118 part20(20)
                                         extensions(0) }

-- a user-friendly name of the subject's eMobility Service Provider
id-contractOperatorName   OBJECT IDENTIFIER := { id-15118-20-ad
                                         contractOperatorName(1) }

END

```

NOTE 6 Refer to ITU-T X.680 for details of ASN.1 notation.

- [V2G20-3054]** If the issuer of the certificate wishes to provide tariff name in the contract certificate, it shall describe the information with one (1) additional access method for 'accessMethod'. Here are the definitions in ASN.1 notation:

```

ISO15118-Extensions { iso(1) standard(0) 15118 part20(20) extensions(0) }
DEFINITIONS :=
BEGIN

id-15118-20-ad          OBJECT IDENTIFIER := { iso(1) standard(0) 15118 part20(20)
                                         extensions(0) }

-- a user-friendly name of the subject's tariff
id-contractTariffName    OBJECT IDENTIFIER := { id-15118-20-ad
                                         contractTariffName(2) }

END

```

NOTE 7 Refer to ITU-T X.680 for details of ASN.1 notation.

- [V2G20-3055]** If the issuer of the certificate wishes to provide dynamic information for the contract, it shall describe the information with one (1) additional access method for 'accessMethod' in the contract certificate. Here are the definitions in ASN.1 notation:

```

ISO15118-Extensions { iso(1) standard(0) 15118 part20(20) extensions(0) }
DEFINITIONS :=
BEGIN

id-15118-20-ad          OBJECT IDENTIFIER := { iso(1) standard(0) 15118 part20(20)
                                         extensions(0) }

-- the URL to a distribution point of (daily) current additional information of the subject's contract
id-contractDynamicInformationUrl  OBJECT IDENTIFIER := { id-15118-20-ad
                                         contractDynamicInformationUrl(3) }

END

```

NOTE 8 Refer to ITU-T X.680 for details of ASN.1 notation.

- [V2G20-3056]** If the issuer of the certificate wishes to provide eMSP name in the contract certificate or provide tariff name in the contract certificate or provide both, the issuer of the certificate shall describe the information with one (1) additional other name for type field in 'otherName'. Here are the definitions in ASN.1 notation:

```

ISO15118-Extensions { iso(1) standard(0) 15118 part20(20) extensions(0) }
DEFINITIONS :=
BEGIN

id-15118-20-ad          OBJECT IDENTIFIER := { iso(1) standard(0) 15118 part20(20)
                                         extensions(0) }

-- an UTF8 string
id-utf8String            OBJECT IDENTIFIER := { id-15118-20-ad utf8String(7) }

END

```

NOTE 9 Refer to ITU-T X.680 for details of ASN.1 notation.

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

As mentioned in Table B.9 and Table B.10, 'SubjectInfoAccess' extension in the contract certificate is optional. Relying parties are not required to ensure that this extension is present in the contract certificate.

Additionally, each accessDescription, i.e. 'accessDescription (ContractMobilityOperatorName)', 'accessDescription (ContractTariffName)' and 'accessDescription (ContractDynamicInformationUrl)', within 'SubjectInfoAccess' extension is also optional. It is left to the local policy of the relying party whether it requires any or all of these accessDescriptions to be present in the contract certificate.

[V2G20-3057] If 'SubjectInfoAccess' extension is present, the relying party shall ensure that one (1) or more accessDescriptions, as defined in Table B.9 or Table B.10, are present.

As mentioned in Table B.9 and Table B.10, 'SubjectInfoAccess' extension in the contract certificate is non-critical. This document does not require the relying parties relying on and/or processing the Contract Certificate to process this extension. It is left to the local policy of the relying party whether it needs to process the 'SubjectInfoAccess' extension (and any information/parameters contained within this extension). It is left to the local policy of the relying party whether it requires any or all of these accessDescriptions in the contract certificate to be processed or not.

ContractDynamicInformationUrl provides a URL to a distribution point of current (daily) additional information to the contract for the customer/EV. This contract information may be downloaded and processed by the EV (or any other IT system managing the contract for the customer/EV). EV may use any methods available to it to download this data. This includes, the internet services (VAS) provided by the EVSE, or any other method available to the EV to reach the provided URL. The usage of the data located at the URL is up to the OEM's implementation.

Clause B.7.1

Replace Table B.11 with this table:

Table B.11 — OEM provisioning certificates based on curves as defined by [V2G20-2674]

ISO 15118-20 certificate profiles		EV manufacturer: OEM provisioning			
		OEM Root CA Root	OEM Sub-CA 1 Sub	OEM Sub-CA 2 Sub	OEM provisioning certificate Leafs
	Version	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)
	SerialNumber	x	x	x	x
Signature	AlgorithmIdentifier	x	x	x	x
	algorithm	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512
	parameters	-	-	-	-

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**
Table B.11 (continued)

ISO 15118-20 certificate profiles			EV manufacturer: OEM provisioning			
		OEM Root CA Root	OEM Sub-CA 1 Sub	OEM Sub-CA 2 Sub	OEM provisioning certificate Leafs	
Issuer	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	
	Organization (O)	x	x	x	x	
	Organization Unit (OU)	(x)	(x)	(x)	(x)	
	Common Name (CN)	x	x	x	x	
	Domain Component (DC)	(x)	(x)	(x)	(x)	
Validity	Validity	x [up to OEM]	x [up to OEM]	x [up to OEM]	x [up to OEM]	
Subject	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	
	Organization (O)	x	x	x	x	
	Organization Unit (OU)	(x)	(x)	(x)	(x)	
	Common Name (CN)	x	x	x	x PCID (see [V2G20-1780])	
	Domain Component (DC)	(x)	(x)	(x)	(x) (shall not end with "EV")	
Subject-PublicKey-Info	AlgorithmIdentifier	x	x	x	x	
	algorithm	x id-ecPublicKey	x id-ecPublicKey	x id-ecPublicKey	x id-ecPublicKey	
	parameters (ECPParameters)	x	x	x	x	
	namedCurve	x secp521r1	x secp521r1	x secp521r1	x secp521r1	
	SubjectPublicKey	x (BIT STRING)	x (BIT STRING)	x (BIT STRING)	x (BIT STRING)	
IssuerUniqueID		-	-	-	-	
SubjectUniqueID		-	-	-	-	
	AuthorityKeyIdentifier	-	x / nc id-ce-authorityKeyIdentifier	x / nc id-ce-authorityKeyIdentifier	x / nc id-ce-authorityKeyIdentifier	
	keyIdentifier	-	x (see [V2G20-1851])	x (see [V2G20-1851])	x (see [V2G20-1851])	

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**
Table B.11 (continued)

ISO 15118-20 certificate profiles		EV manufacturer: OEM provisioning			
		OEM Root CA Root	OEM Sub-CA 1 Sub	OEM Sub-CA 2 Sub	OEM provisioning certificate Leafs
	authorityCertIssuer	-	-	-	-
	authorityCertSerialNumber	-	-	-	-
	SubjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier
	keyIdentifier	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])
	KeyUsage	x / c id-ce-key-Usage	x / c id-ce-key-Usage	x / c id-ce-key-Usage	x / c id-ce-keyUsage
	digitalSignature	0/1	0/1	0/1	1
	nonRepudiation (contentCommitment)	0/1	0/1	0/1	0/1
	keyEncipherment	0/1	0/1	0/1	0/1
	dataEncipherment	0	0	0	0
	keyAgreement	0/1	0/1	0/1	1
	keyCertSign	1	1	1	0
	cRLSign	0	0	0	0
	encipherOnly	0	0	0	0
	decipherOnly	0	0	0	0
	ExtendedKeyUsage	-	-	-	-
	CertificatePolicies	-	(x) / nc	(x) / nc	(x) / nc
	policyInformation	-	x	x	x
	certPolicyId	-	x (OID of the policy)	x (OID of the policy)	x (OID of the policy)
	policyQualifierInfo	-	(x)	(x)	(x)
	policyQualifierId	-	x id-qt-cps	x id-qt-cps	x id-qt-cps
	qualifier	-	x CPSuri	x CPSuri	x CPSuri
	cPSuri	-	x (CPS URI)	x (CPS URI)	x (CPS URI)
	userNotice	-	-	-	-
	policyInformation	-	(x)	(x)	(x)
:	-	:	:	:	:
:	-	:	:	:	:
	policyInformation	-	(x)	(x)	(x)

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.11 (continued)

ISO 15118-20 certificate profiles			EV manufacturer: OEM provisioning			
TbsCertificate	Extensions	OEM Root CA Root	OEM Sub-CA 1 Sub	OEM Sub-CA 2 Sub	OEM provisioning certificate Leafs	
		BasicConstraints	x / c id-ce-basic-Constraints	x / c id-ce-basic-Constraints	x / c id-ce-basic-Constraints	x / c id-ce-basicConstraints
		cA	TRUE	TRUE	TRUE	FALSE
		pathLenConstraint	-	1	0	-
		CRLDistribution-Points (CRL)	-	(x) / nc id-ce-cRLD-istribution-Points	(x) / nc id-ce-cRLD-istribution-Points	(x) / nc id-ce-cRLDistribution-Points
		distributionPoint	-	x	x	x
		distributionPoint-Name	-	(x) (see [V2G20-3038] and B.2.3.2.1)	(x) (see [V2G20-3038] and B.2.3.2.1)	(x) (see [V2G20-3038] and B.2.3.2.1)
		fullName	-	x (in GeneralNames format)	x (in GeneralNames format)	x (in GeneralNames format)
		generalName	-	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]
		nameRelativeToCRLIssuer	-	-	-	-
		reasons	-	-	-	-
		cRLIssuer	-	(x) (see B.2.3.2.1)	(x) (see B.2.3.2.1)	(x) (see B.2.3.2.1)
		distributionPoint	-	-	-	-
		AuthorityInfoAccess	-	(x) / nc id-pe-authorityInfoAccess	(x) / nc id-pe-authorityInfoAccess	(x) / nc id-pe-authorityInfoAccess
		accessDescription (OCSP)	-	x	x	x
		accessMethod	-	x id-ad-ocsp	x id-ad-ocsp	x id-ad-ocsp
		accessLocation	-	x (URI of the OCSP responder)	x (URI of the OCSP responder)	x (URI of the OCSP responder)
		generalName	-	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]
		accessDescription	-	-	-	-

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.11 (continued)**

ISO 15118-20 certificate profiles		OEM Root CA Root	EV manufacturer: OEM provisioning		
		OEM Sub-CA 1 Sub	OEM Sub-CA 2 Sub	OEM provisioning certificate Leafs	
SubjectInfoAccess	accessDescription (TpmStorageKey)	-	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	(x) / nc id-pe-subjectInfoAccess
	accessMethod	-	-	-	x id-tpmStorageKey (see [V2G20-2596])
	accessLocation	-	-	-	x
	generalName	-	-	-	x otherName [0]
	type-id	-	-	-	x id-octetString (see [V2G20-3068])
	value	-	-	-	x (EVCC's TPM public storage key that can be used by the issuing SA to encrypt the newly generated private key so that this information can be stored directly in the EVCC's TPM. Syntax: 132 byte public key in base64 encoding)
accessDescription (TpmPolicyDigest)	accessDescription (TpmPolicyDigest)	-	-	-	x
	accessMethod	-	-	-	x id-tpmPolicyDigest (see [V2G20-2596])
	accessLocation	-	-	-	x
	generalName	-	-	-	x otherName [0]
	type-id	-	-	-	x id-octetString (see [V2G20-3068])

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**
Table B.11 (continued)

ISO 15118-20 certificate profiles		OEM Root CA Root	EV manufacturer: OEM provisioning		
		OEM Sub-CA 1 Sub	OEM Sub-CA 2 Sub	OEM provisioning certificate Leafs	
	value	-	-	-	x (EVCC's TPM policy digest that shall be added to the information generated by the issuing SA before encryption. Syntax: 64 byte hash value in base64 encoding)
	accessDescription (CrossCertIndication)	-	x	x	-
	accessMethod	-	x id-cross-CertIndication (see [V2G20-2604])	x id-cross-CertIndication (see [V2G20-2604])	-
	accessLocation	-	x	x	-
	generalName	-	x otherName [0]	x otherName [0]	-
	type-id	-	x id-utf8String (see [V2G20-3077])	x id-utf8String (see [V2G20-3077])	-
	value	-	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	-
	accessDescription	-	-	-	-
Signature-Algorithm	AlgorithmIdentifier	x	x	x	x
	algorithm	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512
	parameters	-	-	-	-
Signature Value		(Octet-String)	(Octet-String)	(Octet-String)	(Octet-String)

Clause B.7.2

Replace entire text in this clause, and Table B.12 with:

Table B.12 outlines OEM provisioning certificates based on curves as defined by [V2G20-2319].

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.12 — OEM provisioning certificates based on curves as defined by [V2G20-2319]**

		EV manufacturer: OEM provisioning			
		OEM Root CA	OEM Sub-CA 1	OEM Sub-CA 2	OEM provisioning certificate Leafs
ISO 15118-20 certificate profiles	Root	Root	Sub	Sub	
Version	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)
SerialNumber	x	x	x	x	x
Signature	AlgorithmIdentifier algorithm parameters	x id-Edd448 -	x id-Edd448 -	x id-Edd448 -	x id-Edd448 -
Issuer	Organization (O) Organization Unit (OU) Common Name (CN) Domain Component (DC)	(x) x x (x)	(x) x x (x)	(x) x x (x)	(x) x x (x)
Validity	Validity	[up to OEM] (x) Country (C)	[up to OEM] (x) Organization (O) Organization Unit (OU)	[up to OEM] (x) Common Name (CN) Domain Component (DC)	[up to OEM] (x) [up to OEM] (x) Domain Component (DC)
Subject	Common Name (CN) Domain Component (DC)	x (x)	x (x)	x (x)	x PCID (see [V2G20-1780]) (x) (shall not end with "EV")

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.12 (continued)**

ISO 15118-20 certificate profiles		OEM Root CA	EV manufacturer: OEM provisioning certificate	OEM Sub-CA 1	OEM Sub-CA 2	OEM provisioning certificate Leafs
		Root	Sub	Sub	Sub	Leafs
SubjectPublicK-eyInfo	AlgorithmIdentifier	x	x	x	x	x
	algorithm	x	x	x	x	x
	parameters	id-Ed448	id-Ed448	id-Ed448	id-Ed448	id-Ed448
	SubjectPublicKey	x / c (BIT STRING)	x / c (BIT STRING)	x / c (BIT STRING)	x / c (BIT STRING)	x / c (BIT STRING)
	IssuerUniqueID	-	-	-	-	-
SubjectUniqueID	AuthorityKeyIdentifier	-	x / nc id-ce-authorityKey- Identifier	x / nc id-ce-authorityKey- Identifier	x / nc id-ce-authorityKey- Identifier	x / nc id-ce-authorityKey- Identifier
	keyIdentifier	-	x (see [V2G20-1851])	x (see [V2G20-1851])	x (see [V2G20-1851])	x (see [V2G20-1851])
	authorityCertIssuer	-	-	-	-	-
	authorityCertSerialNumber	-	-	-	-	-
	SubjectKeyIdentifier	x / nc id-ce-subject- KeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier
66	keyIdentifier	x (see [V2G20- 1852])	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])
	KeyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage
	digitalSignature	0/1	0/1	0/1	0/1	1
	nonRepudiation (contentCom- mitment)	0/1	0/1	0/1	0/1	0/1
	keyEncipherment	0/1	0/1	0/1	0/1	0/1
Firmenname: Hochschule für Technik, Wirtschaft und Kultur Benutzername: _ip_user_c8563dc5-739d-4631-bf84-0b2da5471fdb	dataEncipherment	0	0	0	0	0
	keyAgreement	0/1	0/1	0/1	0/1	0x
	keyCertSign	1	1	1	1	0

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.12 (continued)**

ISO 15118-20 certificate profiles	EV manufacturer: OEM provisioning			OEM provisioning certificate Leafs
	OEM Root CA Root	OEM Sub-CA 1 Sub	OEM Sub-CA 2 Sub	
cRLSign	0	0	0	0
encipherOnly	0	0	0	0
decipherOnly	0	0	0	0
ExtendedKeyUsage	-	-	-	-
CertificatePolicies	-	(x) / nc	(x) / nc	(x) / nc
policyInformation	-	x	x	x
certPolicyId	-	x (OID of the policy)	x (OID of the policy)	x (OID of the policy)
policyQualifierInfo	-	(x)	(x)	(x)
policyQualifierId	-	x id-qt-cps	x id-qt-cps	x id-qt-cps
qualifier	-	x CPSuri	x CPSuri	x CPSuri
CPSuri	-	x (CPS URI)	x (CPS URI)	x (CPS URI)
userNotice	-	-	-	-
policyInformation	-	(x)	(x)	(x)
:	-	:	:	:
:	-	:	:	:
policyInformation	-	(x)	(x)	(x)
BasicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints
cA	TRUE	TRUE	TRUE	FALSE
pathLenConstraint	-	1	0	-
CRLDistributionPoints (CRL)	-	id-ce-cRLDistributionPoints	(x) / nc id-ce-cRLDistributionPoints	(x) / nc id-ce-cRLDistributionPoints
distributionPoint	-	x	x	x

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.12 (continued)**

		EV manufacturer: OEM provisioning certificate			OEM provisioning certificate Leafs
		OEM Root CA	OEM Sub-CA 1	OEM Sub-CA 2	
		Root	Sub	Sub	
TbsCertificate	distributionPointName	-	(see [V2G20-3038] and B.2.3.2.1)	(see [V2G20-3038] and B.2.3.2.1)	(see [V2G20-3038] and B.2.3.2.1)
	fullName	-	x (in GeneralNames format)	x (in GeneralNames format)	x (in GeneralNames format)
	generalName	-	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]
	nameRelativeToCRLIssuer	-	-	-	-
	reasons	-	-	-	-
	cRLIssuer	-	(x) (see B.2.3.2.1)	(x) (see B.2.3.2.1)	(x) (see B.2.3.2.1)
	distributionPoint	-	-	-	-
	AuthorityInfoAccess	-	(x) / nc id-pe-authorityInfoAccess	(x) / nc id-pe-authorityInfoAccess	(x) / nc id-pe-authorityInfoAccess
	accessDescription (OCSP)	-	x id-ad-ocsp	x id-ad-ocsp	x id-ad-ocsp
	accessMethod	-	x (URI of the OCSP responder)	x (URI of the OCSP responder)	x (URI of the OCSP responder)
Extensions	accessLocation	-	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]
	generalName	-	-	-	-
Extensions	accessDescription	-	-	-	-

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.12 (continued)

ISO 15118-20 certificate profiles	OEM Root CA	EV manufacturer: OEM provisioning		OEM provisioning certificate Leafs
	Root	OEM Sub-CA 1	OEM Sub-CA 2	Sub
SubjectInfoAccess		(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])
accessDescription (x448Pub- licKey)	-	-	-	x
accessMethod	-	-	-	x id-x448PpublicKey (see [V2G20-3063])
accessLocation	-	-	-	x
generalName	-	-	-	x otherName [0]
type-id	-	-	-	x id-bitString (see [V2G20-3064])
value				x (x448 public key to be used for ECDHE key agree- ment per 7.9.2.5.4). Syntax: 56 byte BIT STRING)
accessDescription (TpmStor- ageKey)	-	-	-	(x)
accessMethod	-	-	-	x id-tpmStorageKey (see [V2G20-2596])
accessLocation	-	-	-	x
generalName				x otherName [0]

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.12 (continued)

ISO 15118-20 certificate profiles	EV manufacturer: OEM provisioning			
	OEM Root CA Root	OEM Sub-CA 1 Sub	OEM Sub-CA 2 Sub	OEM provisioning cer- tificate Leafs
type-id	-	-	-	x id-octetString (see [V2G20-3068])
value	-	-	-	(EVCC's TPM public storage key that can be used by the issuing SA to encrypt the newly generated private key so that this information can be stored directly in the EVCC's TPM. Syntax: 132 byte public key in base64 encoding)
accessDescription (TpmPol- icyDigest)	-	-	-	(x)
accessMethod	-	-	-	x id-tpmPolicyDigest (see [V2G20-2596])
accessLocation	-	-	-	x
generalName	-	-	-	x otherName [0]
type-id	-	-	-	x id-octetString (see [V2G20-3068])
value	-	-	-	x (EVCC's TPM policy digest that shall be added to the information generated by the issuing SA before encryption. Syntax: 64 byte hash value in base64 encoding)

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.12 (continued)**

		EV manufacturer: OEM provisioning			OEM provisioning certificate Leafs
		OEM Root CA Root	OEM Sub-CA 1 Sub	OEM Sub-CA 2 Sub	
ISO 15118-20 certificate profiles	accessDescription (Cross-CertIndication)	-	x	x	-
	accessMethod	-	x id-crossCertIndication (see [V2G20-2604])	x id-crossCertIndication (see [V2G20-2604])	-
	accessLocation	-	x	x	-
	generalName	-	x otherName [0]	x otherName [0]	-
	type-id	-	x id-utf8String (see [V2G20-3077])	x id-utf8String (see [V2G20-3077])	-
	value	-	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	-
	accessDescription	-	-	-	-
SignatureAlgorithm	AlgorithmIdentifier	x	x	x	x
	algorithm	x id-Ed448	x id-Ed448	x id-Ed448	x id-Ed448
	parameters	-	-	-	-
	Signature Value	(Raw BIT STRING)	(Raw BIT STRING)	(Raw BIT STRING)	(Raw BIT STRING)

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

- [V2G20-3058]** For “Contract Transport Public Key” used for ECDHE in 7.9.2.5.4, the EVCC shall generate a new public/private key pair using the curve448 as defined by IETF RFC 7748, sections 5 and 6.2.

NOTE 1 Due to possibility of issues with the birational maps, the EVCC should not use them to convert the edward448 public key to curve448. The EVCC should, rather, generate a separate curve448 public/private key pair.

NOTE 2 This means that the EVCC will need to maintain a second private key for OEM provisioning certificate. The EVCC will use this curve448 (second) private key for calculation of the decryption key per 7.9.2.5.4.

[V2G20-3059] The ‘value’ field of ‘generalName’ parameter of ‘accessLocation’ field of ‘accessDescription (x448PublicKey)’ parameter in the extension ‘subjectInfoAccess’ of in the OEM provisioning certificate shall contain the public key created using

As mentioned in Table B.12, ‘subjectInfoAccess’ extension in the OEM provisioning certificate is non-critical.

- [V2G20-3060]** All relying parties shall process ‘subjectInfoAccess’ extension in the OEM provisioning certificate.

- [V2G20-3061]** The relying parties shall not use the “Contract Transport Public Key” contained in the ‘value’ field of ‘generalName’ parameter of ‘accessLocation’ field of ‘accessDescription (x448PublicKey)’ parameter in the extension ‘subjectInfoAccess’ in the OEM provisioning certificate for any purpose other than ECDHE.

- [V2G20-3062]** The relying parties shall have controls in place to ensure that “Contract Transport Public Key” contained in the ‘value’ field of ‘generalName’ parameter of ‘accessLocation’ field of ‘accessDescription (x448PublicKey)’ parameter in the extension ‘subjectInfoAccess’ in the OEM provisioning certificate can only be used for ECDHE.

NOTE 1 The controls specified by [V2G20-2593] could be similar ones as used when KeyUsage extension restrictions are applied to the public key in the certificates.

NOTE 2 For example, when processing the “Contract Transport Public Key” contained in the ‘value’ field of ‘generalName’ parameter of ‘accessLocation’ field of ‘accessDescription (x448PublicKey)’ parameter in the extension ‘subjectInfoAccess’, the relying party will assume as if digitalSignature flag in KeyUsage extension is set to 0, nonRepudiation (contentCommitment) flag in KeyUsage extension is set to 0, keyEncipherment flag in KeyUsage extension is set to 0, dataEncipherment flag in KeyUsage extension is set to 0, keyAgreement flag in KeyUsage extension is set to 1, keyCertSign flag in KeyUsage extension is set to 0, cRLSign flag in KeyUsage extension is set to 0, encipherOnly flag in KeyUsage extension is set to 0 and decipherOnly flag in KeyUsage extension is set to 0,

- [V2G20-3063]** The issuer of the certificate shall describe the information with one (1) additional access description for "AccessDescription". Here are the definitions in ASN.1 notation:

```
ISO15118-Extensions { iso(1) standard(0) 15118 part20(20) extensions(0) }
DEFINITIONS :=
BEGIN
id-15118-20-ad OBJECT IDENTIFIER := { iso(1) standard(0) 15118 part20(20)
                                         extensions(0) }

-- x448 Public Key for ECDHE
id-x448PublicKey OBJECT IDENTIFIER := { id-15118-20-ad x448PublicKey(9) }

END
```

NOTE 3 Refer to ITU-T X.680 for details of ASN.1 notation.

- [V2G20-3064]** The issuer of the OEM Provisioning Certificate shall describe the information with one (1) additional other name for type field in ‘otherName’. Here are the definitions in ASN.1 notation:

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

```

ISO15118-Extensions { iso(1) standard(0) 15118 part20(20) extensions(0) }
DEFINITIONS :=
BEGIN

id-15118-20-ad          OBJECT IDENTIFIER := { iso(1) standard(0) 15118 part20(20)
                                                extensions(0) }

-- a bit string
id-bitString              OBJECT IDENTIFIER := { id-15118-20-ad bitString(10) }

END

```

NOTE 4 Refer to ITU-T X.680 for details of ASN.1 notation.

Clause B.7.3

Replace entire text in this clause with:

As mentioned in Table B.11 and Table B.12 it is optional to include the ‘certificatePolicies’ extension in any of the OEM provisioning certificates. If the ‘certificatePolicies’ extension is included, it can be marked as non-critical so that, if allowed by the local policy, the relying party can ignore this extension if it cannot process it. This is done to improve the interoperability.

It should be noted that neither EVCC nor SECC validate the OEM provisioning certificate or any other certificates included in that chain. The EVCC provides this certificate to the eMSP during CertificateInstallationReq. It is up to the eMSP to validate the certificate and ensure it meets the requirements.

When the configurable mechanism as defined by [V2G20-2320] indicates that the curve as defined by [V2G20-2319] needs to be used, the EVCC will send its OEM provisioning certificate conforming to Table B.11 to the eMSP via the SECC. When the configurable mechanism as defined by [V2G20-2320] indicates that the curve as defined by [V2G20-2674] needs to be used, the EVCC will send its OEM provisioning certificate conforming to Table B.12 to the eMSP via the SECC. When the eMSP receives an OEM provisioning certificate conforming to Table B.12, it will use SubjectPublicKey defined in Table B.11 for ECDHE per 7.9.2.5.4. When the eMSP receives an OEM provisioning certificate conforming to Table B.12, it will use “Contract Transport Public Key” contained in the ‘value’ field of ‘generalName’ parameter of ‘accessLocation’ field of ‘accessDescription (x448PublicKey)’ parameter in the extension ‘subjectInfoAccess’ in the OEM provisioning certificate defined in Table B.12 for ECDHE per 7.9.2.5.4.

[V2G20-1780] PCID shall be created per C.2.

[V2G20-1781] PCID shall be contained in the subject field of the provisioning certificate as follows:

- The PCID itself (see [V2G20-1780]) shall be the value of the common name (CN) of the distinguished name (DN).
- The name of the OEM shall be encoded in the field organization (O) using a unique identifier chosen by the OEM, to identify this OEM.
- The X.500 distinguished name in the subject field shall not contain any further values.

[V2G20-3065] Subject field of the OEM Provisioning Certificate shall not contain Domain Component ending with “EV”.

[V2G20-3066] The CA, at its discretion, may include any other necessary information in the Domain Component RDN of the Subject field of the OEM Provisioning Certificate without violating **[V2G20-3065]**.

[V2G20-2592] OEM Sub CA1 certificate, OEM Sub CA2 certificate and OEM provisioning certificate shall contain either ‘CRLDistributionPoints’ extension or ‘AuthorityInfoAccess’ extension or both.

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

NOTE 1 Table B.11 and Table B.12 specify that both ‘CRLDistributionPoints’ and ‘AuthorityInfoAccess’ extensions are optional to indicate that either one of them can be included. [V2G20-2592] clarifies that including at least one of them is mandatory while including both of them is not mandatory.

NOTE 2 [V2G20-2592] does not specify which one of these extensions can be included. It is left up to the OEM to decide which certificate revocation method works best for it. In some cases CRLs will work better as they allow the relying party to download the entire CRL once and have it available for local checking of revocation status of the next OEM provisioning certificate without a need for a live connection to the CRL server while in other cases OCSP will provide better results as it provides current revocation status and requires less storage and searching on part of the relying party.

[V2G20-2593] If OEM Sub CA1 Certificate or OEM Sub CA2 Certificate or OEM Provisioning Certificate contains both CRLDistributionPoints and AuthorityInfoAccess extensions, the relying party may process just one or both as per the local policy of the relying party. However, the relying party shall process at least one of these extensions.

NOTE 3 Table B.11 and Table B.12 specify that both ‘CRLDistributionPoints’ and ‘AuthorityInfoAccess’ extensions are optional to indicate that at least one of them is included. [V2G20-2593] clarifies that if the issuer desires to include both, it is up to the relying party to decide which one to process. [V2G20-2593] also ensures that the relying party will process at least one.

[V2G20-3067] If OEM Sub CA1 Certificate or OEM Sub CA2 Certificate or OEM Provisioning Certificate contains only one of ‘CRLDistributionPoints’ and ‘AuthorityInfoAccess’ extensions, the relying party shall process the extension that is present.

NOTE 4 Table B.11 and Table B.12 specify that both ‘CRLDistributionPoints’ and ‘AuthorityInfoAccess’ extensions are optional and [V2G20-2593] specifies that it is mandatory to include at least one of them. [V2G20-2591] ensures that, if only one of them is included, the relying party will process that one.

[V2G20-2594] The OEM Provisioning Certificate extensions in Table B.11 and Table B.12 shall use the definition of ‘SubjectInfoAccess’ as defined in IETF RFC 5280, 4.2.2.2, so that the issuer of an OEM Provisioning Certificate can indicate to the eMSP that the EVCC uses a TPM and provide the necessary information to the eMSP to generate the contract certificates and encrypt the associated private key for the TPM. As mentioned in IETF RFC 5280, the field ‘accessMethod’ indicates the type of information and the field ‘accessLocation’ indicates either the information itself or a storage location for the information.

NOTE 5 IETF RFC 5280 has been updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399. These updates are considered to be included in this document.

[V2G20-2595] In case the OEM provisioning certificate provided by/for the EVCC contains the non-critical extension ‘SubjectInfoAccess’ with ‘accessDescription (TpmStorageKey)’ and ‘accessDescription (TpmPolicyDigest)’ fields, the SA/eMSP shall use the method described in 7.9.2.5.3 to encrypt the private contract certificate key for this EVCC.

[V2G20-2596] If the EVCC uses a TPM, the issuer of the OEM Provisioning Certificate shall describe the information with two (2) additional access methods for ‘accessMethod’. Here are the definitions in ASN.1 notation:

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

```

ISO15118-Extensions { iso(1) standard(0) 15118 part20(20) extensions(0) }
DEFINITIONS :=
BEGIN

id-15118-20-ad           OBJECT IDENTIFIER := { iso(1) standard(0) 15118 part20(20)
                                                 extensions(0) }

-- Public Storage Key of EVCC's TPM
id-tpmStorageKey          OBJECT IDENTIFIER := { id-15118-20-ad tpmStorageKey(4) }

-- Policy Digest for EVCC's TPM Contract Keys
id-tpmPolicyDigest         OBJECT IDENTIFIER := { id-15118-20-ad tpmPolicyDigest
                                                 (5) }

...

```

NOTE 6 Refer to ITU-T X.680 for details of ASN.1 notation.

- [V2G20-3068]** The issuer of the OEM Provisioning Certificate shall describe the information with one (1) additional other name for type field in 'otherName'. Here are the definitions in ASN.1 notation:

```

ISO15118-Extensions { iso(1) standard(0) 15118 part20(20) extensions(0) }
DEFINITIONS :=
BEGIN

id-15118-20-ad           OBJECT IDENTIFIER := { iso(1) standard(0) 15118
                                                 part20(20)
                                                 extensions(0) }

-- an octet string
id-octetString            OBJECT IDENTIFIER := { id-15118-20-ad octetString(8) }

...

```

NOTE 7 Refer to ITU-T X.680 for details of ASN.1 notation.

As mentioned in Table B.11 and Table B.12, 'SubjectInfoAccess' extension in the OEM provisioning certificate is optional. Relying parties relying on the OEM provisioning certificate are not required to ensure that this extension is present in the OEM provisioning certificate.

- [V2G20-3069]** EVCC not using a TPM shall not include 'SubjectInfoAccess' extension, as defined in Table B.11 or Table B.12, in its OEM provisioning certificate based on curves as defined by [V2G20-2674].

NOTE 8 OEM provisioning certificate based on curves as defined by [V2G20-2319] will always contain 'SubjectInfoAccess' extension with the "Contract Transport Public Key".

- [V2G20-3070]** EVCC using a TPM shall include 'SubjectInfoAccess' extension, as defined in Table B.11, in its OEM provisioning certificate based on curves as defined by [V2G20-2674]. EVCC using a TPM shall include additional 'accessDescriptions' in the 'SubjectInfoAccess' extension, as defined in Table B.12, in its OEM provisioning certificate based on curves as defined by [V2G20-2319].

- [V2G20-3071]** If 'SubjectInfoAccess' extension is present in the OEM provisioning certificate, the relying party relying on the OEM provisioning certificate based on curves as defined by [V2G20-2674] shall ensure that both 'accessDescription (TpmStorageKey)' and 'accessDescription (TpmPolicyDigest)', as defined in Table B.11, are present. The relying party relying on the OEM provisioning certificate based on curves as defined by [V2G20-2319] shall ensure that either both 'accessDescription (TpmStorageKey)' and 'accessDescription (TpmPolicyDigest)', as defined in Table B.12, are present or both are absent in 'SubjectInfoAccess' extension.

NOTE 9 [V2G20-2593] means that certificate validation of an OEM provisioning certificate with only 'accessDescription (TpmStorageKey)' or 'accessDescription (TpmPolicyDigest)' in the 'SubjectInfoAccess' extension will fail.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

[V2G20-3072] If ‘SubjectInfoAccess’ extension is present in the OEM provisioning certificate, the relying party relying on the OEM provisioning certificate shall process this extension (and any information/parameters contained within this extension).

NOTE 10 ‘SubjectInfoAccess’ extension in the OEM provisioning certificate is marked as non-critical only to comply with requirements as specified by IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399). This requirement ensures that, if this extension is present in the OEM provisioning certificate, it will be processed.

Clause B.8.1

Replace Table B.13 with this table:

Table B.13 — Vehicle certificates based on curves as defined by [V2G20-2674]

ISO 15118-20 certificate profiles		EV manufacturer: vehicle certificates		
		Vehicle Sub-CA 1 Sub	Vehicle Sub-CA 2 Sub	Vehicle certificate Leaf
Version		2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)
SerialNumber		x	x	x
Signature	AlgorithmIdentifier	x	x	x
	algorithm	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512
	parameters	-	-	-
Issuer	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)
	Common Name (CN)	x	x	x
	Domain Component (DC)	(x)	(x)	(x)
Validity	Validity	x [up to OEM]	x [up to OEM]	x [up to OEM]
Subject	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)
	Common Name (CN)	x	x	x EVCCID (see [V2G20-2597])
	Domain Component (DC)	(x)	(x)	(x) & "EV"

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.13 (continued)

ISO 15118-20 certificate profiles		EV manufacturer: vehicle certificates		
		Vehicle Sub-CA 1 Sub	Vehicle Sub-CA 2 Sub	Vehicle certificate Leaf
Subject-PublicKey-Info	AlgorithmIdentifier	x	x	x
	algorithm	x id-ecPublicKey	x id-ecPublicKey	x id-ecPublicKey
	parameters (ECParameters)	x	x	x
	namedCurve	x secp521r1	x secp521r1	x secp521r1
	SubjectPublicKey	x (BIT STRING)	x (BIT STRING)	x (BIT STRING)
	IssuerUniqueID	-	-	-
	SubjectUniqueID	-	-	-
	AuthorityKeyIdentifier	x / nc id-ce-authorityKey-Identifier	x / nc id-ce-authorityKey-Identifier	x / nc id-ce-authorityKey-Identifier
	keyIdentifier	x (see [V2G20-1851])	x (see [V2G20-1851])	x (see [V2G20-1851])
	authorityCertIssuer	-	-	-
TbsCertificate	authorityCertSerialNumber	-	-	-
	SubjectKeyIden-tifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier
	keyIdentifier	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])
	KeyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage
	digitalSignature	0/1	0/1	1
	nonRepudiation (contentCommitment)	0/1	0/1	0/1
	keyEncipherment	0/1	0/1	0/1
	dataEncipherment	0	0	0
	keyAgreement	0/1	0/1	0/1
	keyCertSign	1	1	0
	cRLSign	0	0	0
	encipherOnly	0	0	0
	decipherOnly	0	0	0
	ExtendedKeyUsage	-	-	x / c id-ce-extKeyUsage
	keyPurposeId	-	-	x id-kp-clientAuth
	CertificatePolicies	(x) / nc	(x) / nc	(x) / nc
	policyInformation	x	x	x

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.13 (continued)

ISO 15118-20 certificate profiles		EV manufacturer: vehicle certificates		
		Vehicle Sub-CA 1 Sub	Vehicle Sub-CA 2 Sub	Vehicle certificate Leaf
Extensions	certPolicyId	x (OID of the policy)	x (OID of the policy)	x (OID of the policy)
	policyQualifierInfo	(x)	(x)	(x)
	policyQualifierId	x id-qt-cps	x id-qt-cps	x id-qt-cps
	qualifier	x CPSuri	x CPSuri	x CPSuri
	cPSuri	x (CPS URI)	x (CPS URI)	x (CPS URI)
	userNotice	-	-	-
	policyInformation	(x)	(x)	(x)
	:	:	:	:
	:	:	:	:
	policyInformation	(x)	(x)	(x)
	BasicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints
	cA	TRUE	TRUE	FALSE
	pathLenConstraint	1	0	-
	CRLDistribution-Points (CRL)	(x) / nc id-ce-cRLDistribution-Points	(x) / nc id-ce-cRLDistribution-Points	(x) / nc id-ce-cRLDistributionPoints
	distributionPoint	x	x	x
	distributionPoint-Name	(x) (see [V2G20-3038] and B.2.3.2.1)	(x) (see [V2G20-3038] and B.2.3.2.1)	(x) (see [V2G20-3038] and B.2.3.2.1)
	fullName	x (in GeneralNames format)	x (in GeneralNames format)	x (in GeneralNames format)
	generalName	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]
	nameRelativeToCRLIssuer	-	-	-
	reasons	-	-	-
	cRLIssuer	(x) (see B.2.3.2.1)	(x) (see B.2.3.2.1)	(x) (see B.2.3.2.1)
	distributionPoint	-	-	-
	AuthorityInfoAccess	(x) / nc id-pe-authorityInfoAccess	(x) / nc id-pe-authorityInfoAccess	(x) / nc id-pe-authorityInfoAccess
	accessDescription (OCSP)	x	x	x
	accessMethod	x id-ad-ocsp	x id-ad-ocsp	x id-ad-ocsp

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.13 (continued)

ISO 15118-20 certificate profiles		EV manufacturer: vehicle certificates		
		Vehicle Sub-CA 1 Sub	Vehicle Sub-CA 2 Sub	Vehicle certificate Leaf
Signature-Algorithm	accessLocation	x (URI of the OCSP responder)	x (URI of the OCSP responder)	x (URI of the OCSP responder)
	generalName	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]
	accessDescription	-	-	-
	SubjectInfoAccess	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	-
	accessDescription (CrossCertIndication)	x	x	-
	accessMethod	x id-crossCertIndication (see [V2G20-2604])	x id-crossCertIndication (see [V2G20-2604])	-
	accessLocation	x	x	-
	generalName	x otherName [0]	x otherName [0]	-
	type-id	x id-utf8String (see [V2G20-3077])	x id-utf8String (see [V2G20-3077])	-
	value	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	-
accessDescription		-	-	-
Signature Value	AlgorithmIdentifier	x	x	x
	algorithm	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512
	parameters	-	-	-

Delete NOTE 1 and NOTE 3 below Table B.13 and renumber NOTE 2.

Clause B.8.2

Replace Table B.14 with this table:

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.14 — Vehicle certificates based on curves as defined by [V2G20-2319]

ISO 15118-20 certificate profiles		EV manufacturer: vehicle certificates		
		Vehicle Sub-CA 1 Sub	Vehicle Sub-CA 2 Sub	Vehicle certificate Leaf
Version		2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)
SerialNumber		x	x	x
Signature	AlgorithmIdentifier	x	x	x
	algorithm	x id-Ed448	x id-Ed448	x id-Ed448
	parameters	-	-	-
Issuer	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)
	Common Name (CN)	x	x	x
	Domain Component (DC)	(x)	(x)	(x)
Validity	Validity	x [up to OEM]	x [up to OEM]	x [up to OEM]
Subject	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)
	Common Name (CN)	x	x	x EVCCID (see [V2G20-2597])
	Domain Component (DC)	(x)	(x)	(x) & "EV"
Subject-PublicKey-Info	AlgorithmIdentifier	x	x	x
	algorithm	x id-Ed448	x id-Ed448	x id-Ed448
	parameters	-	-	-
	SubjectPublicKey	x (BIT STRING)	x (BIT STRING)	x (BIT STRING)
IssuerUniqueID		-	-	-
SubjectUniqueID		-	-	-
	AuthorityKeyIdentifier	x / nc id-ce-authorityKey-Identifier	x / nc id-ce-authorityKey-Identifier	x / nc id-ce-authorityKey-Identifier
	keyIdentifier	x (see [V2G20-1851])	x (see [V2G20-1851])	x (see [V2G20-1851])

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.14 (continued)

ISO 15118-20 certificate profiles		EV manufacturer: vehicle certificates		
		Vehicle Sub-CA 1 Sub	Vehicle Sub-CA 2 Sub	Vehicle certificate Leaf
TbsCertificate	authorityCertIssuer	-	-	-
	authorityCertSerialNumber	-	-	-
	SubjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier
	keyIdentifier	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])
	KeyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage
	digitalSignature	0/1	0/1	1
	nonRepudiation (contentCommitment)	0/1	0/1	0/1
	keyEncipherment	0/1	0/1	0/1
	dataEncipherment	0	0	0
	keyAgreement	0/1	0/1	0/1
	keyCertSign	1	1	0
	cRLSign	0	0	0
	encipherOnly	0	0	0
	decipherOnly	0	0	0
	ExtendedKeyUsage	-	-	x / c id-ce-extKeyUsage
	keyPurposeId	-	-	x id-kp-clientAuth
	keyPurposeId	-	-	(x) id-kp-serverAuth
	CertificatePolicies	(x) / nc	(x) / nc	(x) / nc
	policyInformation	x	x	x
	certPolicyId	x (OID of the policy)	x (OID of the policy)	x (OID of the policy)
	policyQualifierInfo	(x)	(x)	(x)
	policyQualifierId	x id-qt-cps	x id-qt-cps	x id-qt-cps
	qualifier	x CPSuri	x CPSuri	x CPSuri
	cPSuri	x (CPS URI)	x (CPS URI)	x (CPS URI)
	userNotice	-	-	-
	policyInformation	(x)	(x)	(x)
	:	:	:	:
	:	:	:	:
	policyInformation	(x)	(x)	(x)

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.14 (continued)

ISO 15118-20 certificate profiles		EV manufacturer: vehicle certificates		
		Vehicle Sub-CA 1 Sub	Vehicle Sub-CA 2 Sub	Vehicle certificate Leaf
Extensions	BasicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints
	cA	TRUE	TRUE	FALSE
	pathLenConstraint	1	0	-
	CRLDistribution- Points (CRL)	(x) / nc id-ce-cRLDistribution- Points	(x) / nc id-ce-cRLDistribution- Points	(x) / nc id-ce-cRLDistribu- tionPoints
	distributionPoint	x	x	x
	distributionPoint- Name	(x) (see [V2G20-3038] and B.2.3.2.1)	(x) (see [V2G20-3038] and B.2.3.2.1)	(x) (see [V2G20-3038] and B.2.3.2.1)
	fullName	x (in GeneralNames format)	x (in GeneralNames format)	x (in GeneralNames format)
	generalName	x uniformResourceIden- tifier [6]	x uniformResourceIden- tifier [6]	x uniformResourcel- dentifier [6]
	nameRela- tiveToCRLIssuer	-	-	-
	reasons	-	-	-
	cRLIssuer	(x) (see B.2.3.2.1)	(x) (see B.2.3.2.1)	(x) (see B.2.3.2.1)
	distributionPoint	-	-	-
	AuthorityInfoAc- cess	(x) / nc id-pe-authorityInfoAc- cess	(x) / nc id-pe-authorityInfoAc- cess	(x) / nc id-pe-authorityIn- foAccess
	accessDescription (OCSP)	x	x	x
	accessMethod	x id-ad-ocsp	x id-ad-ocsp	x id-ad-ocsp
	accessLocation	x (URI of the OCSP re- sponder)	x (URI of the OCSP re- sponder)	x (URI of the OCSP responder)
	generalName	x uniformResourceIden- tifier [6]	x uniformResourceIden- tifier [6]	x uniformResourceI- dentifier [6]
	accessDescription	-	-	-
	SubjectInfoAccess	(x) / nc id-pe-subjectInfoAc- cess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	(x) / nc id-pe-subjectInfoAc- cess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	-
	accessDescription (CrossCertIndica- tion)	x	x	-

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**
Table B.14 (continued)

ISO 15118-20 certificate profiles		EV manufacturer: vehicle certificates		
		Vehicle Sub-CA 1 Sub	Vehicle Sub-CA 2 Sub	Vehicle certificate Leaf
	accessMethod	x id-crossCertIndication (see [V2G20-2604])	x id-crossCertIndication (see [V2G20-2604])	-
	accessLocation	x	x	-
	generalName	x otherName [0]	x otherName [0]	-
	type-id	x id-utf8String (see [V2G20-3077])	x id-utf8String (see [V2G20-3077])	-
	value	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	-
	accessDescription	-	-	-
Signature-Algorithm	AlgorithmIdentifier	x	x	x
	algorithm	x id-Ed448	x id-Ed448	x id-Ed448
	parameters	-	-	-
Signature Value		(Raw BIT STRING)	(Raw BIT STRING)	(Raw BIT STRING)

Delete NOTE below Table B.14.

Clause B.8.3

Replace entire text in this clause with:

As mentioned in Table B.13 and Table B.14, it is optional to include the ‘certificatePolicies’ extension in any of the vehicle certificates. If the ‘certificatePolicies’ extension is included, it can be marked as non-critical so that, if allowed by the local policy, the relying party can ignore this extension if it cannot process it. This is done to improve the interoperability.

[V2G20-2597] EVCCID shall be created per C.5.

[V2G20-2598] EVCCID shall be contained in the subject field of the Vehicle Certificate as follows:

- The EVCCID itself (see [V2G20-2597]) shall be the value of the Common Name (CN) of the Distinguished Name (DN).
- The name of the OEM shall be encoded in the field Organization (O) using a unique identifier chosen by the OEM, to identify this OEM.
- The X.500 distinguished name in the subject field shall not contain any further values.

[V2G20-3073] Subject field of the Vehicle Certificate shall contain Domain Component ending with “EV”.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

[V2G20-3074] The CA, at its discretion, may include any other necessary information in the Domain Component RDN of the Subject field of the Vehicle Certificate without violating **[V2G20-3073]**.

[V2G20-2599] Vehicle Sub CA1 Certificate, Vehicle Sub CA2 Certificate and Vehicle Certificate shall contain either 'CRLDistributionPoints' extension or 'AuthorityInfoAccess' extension or both.

NOTE 1 Table B.13 and Table B.14 specify that both 'CRLDistributionPoints' and 'AuthorityInfoAccess' extensions are optional to indicate that either one of them can be included. [V2G20-2599] clarifies that including at least one of them is mandatory while including both of them is not mandatory.

NOTE 2 [V2G20-2599] does not specify which one of these extensions can be included. It is left up to the OEM to decide which certificate revocation method works best for it. In some cases CRLs will work better as they allow the relying party to download the entire CRL once and have it available for local checking of revocation status of the next vehicle certificate without a need for a live connection to the CRL server while in other cases OCSP will provide better results as it provides current revocation status and requires less storage and searching on part of the relying party.

[V2G20-2600] If Vehicle Sub CA1 certificate or Vehicle Sub CA2 certificate or Vehicle certificate contains both 'CRLDistributionPoints' and 'AuthorityInfoAccess' extensions, the relying party may process just one or both as per the local policy of the relying party. However, the relying party shall process at least one of these extensions.

NOTE 3 Table B.13 and Table B.14 specify that both 'CRLDistributionPoints' and 'AuthorityInfoAccess' extensions are optional to indicate that at least one of them is included. [V2G20-2600] clarifies that if the issuer desires to include both, it is up to the relying party to decide which one to process. [V2G20-2600] also ensures that the relying party will process at least one.

[V2G20-3075] If Vehicle Sub CA1 Certificate or Vehicle Sub CA2 Certificate or Vehicle Certificate contains only one of 'CRLDistributionPoints' and 'AuthorityInfoAccess' extensions, the relying party shall process the extension that is present.

NOTE 4 Table B.13 and Table B.14 specify that both 'CRLDistributionPoints' and 'AuthorityInfoAccess' extensions are optional and [V2G20-2599] specifies that it is mandatory to include at least one of them. [V2G20-3075] ensures that, if only one of them is included, the relying party will process that one.

There may be use cases allowing usage of vehicle certificate for both client and server authentication. As such, the vehicle certificate profile provides for the possibility of allowing the vehicle certificate to be used for both. Since these use cases are not fully defined yet, it is left up to the OEM's discretion whether to generate vehicle certificates that can be used for both client and server authentication or those that can only be used for client authentication.

To allow widest acceptance of the vehicle certificate, vehicle certificates should be derived from a chain originating from a V2G Root CA certificate. This allows the SECC to validate the vehicle certificate using a V2G Root that it may possess. If the vehicle certificates cannot be derived from a chain originating from a V2G Root CA certificate, the vehicle certificate chain may be cross signed by a V2G Root CA certificate. Refer to H.1.5 and its subclauses for further details on cross-signing.

Clause B.9

Replace Title of B.9 with this Title:

B.9 Cross certificate & OCSP signer/responder certificate profiles

Clause B.9.1

Replace entire text in this clause, and Table B.15 with:

Table B.15 outlines the cross certificate and OCSP signer/responder certificate based on curves as defined by [V2G20-2674].

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.15 — Cross certificate and OCSP signer/responder certificate based on curves as defined by [V2G20-2674]

ISO 15118-20 certificate profiles		Cross cross certificate	OCSP OCSP signer/responder certificate
	Version	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)
	SerialNumber	x	x
Signature	AlgorithmIdentifier	x	x
	algorithm	x ecdsa-with-SHA512	x ecdsa-with-SHA512
	parameters	-	-
Issuer	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x
	Organization Unit (OU)	(x)	(x)
	Common Name (CN)	x	x
	Domain Component (DC)	(x)	(x)
Validity	Validity	x [up to issuer]	x [up to 1 year]
Subject	Country (C)	(x) (ISO 3166-1 alpha-2 code)	-
	Organization (O)	x	x
	Organization Unit (OU)	(x)	(x)
	Common Name (CN)	x	x
	Domain Component (DC)	(x)	(x)
SubjectPub-licKeyInfo	AlgorithmIdentifier	x	x
	algorithm	x id-ecPublicKey	x id-ecPublicKey
	parameters (ECPa-rameters)	x	x
	namedCurve	x secp521r1	x secp521r1
	SubjectPublicKey	x (BIT STRING)	x (BIT STRING)
IssuerUniqueID		-	-
SubjectUniqueID		-	-
	AuthorityKeyIdentifier	x / nc id-ce-authorityKey-Identifier	x / nc id-ce-authorityKey-Identifier
	keyIdentifier	x (see [V2G20-1851])	x (see [V2G20-1851])
	authorityCertIssuer	-	-

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.15 (continued)**

ISO 15118-20 certificate profiles		Cross cross certificate	OCSP OCSP signer/re- sponder certificate
TbsCertificate	authorityCertSerialNumber	-	-
	SubjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier
	keyIdentifier	x (see [V2G20-1852])	x (see [V2G20-1852])
	KeyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage
	digitalSignature	0/1	0/1
	nonRepudiation (contentCommitment)	0/1	0/1
	keyEncipherment	0/1	0/1
	dataEncipherment	0	0
	keyAgreement	0/1	0
	keyCertSign	1	0
	cRLSign	0/1	0
	encipherOnly	0	0
	decipherOnly	0	0
	ExtendedKeyUsage	-	x / c id-ce-extKeyUsage
	keyPurposeId	-	x id-kp-OCSPSigning
	CertificatePolicies	(x) / nc	(x) / nc
	policyInformation	x	x
	certPolicyId	x (OID of the policy)	x (OID of the policy)
	policyQualifierInfo	(x)	(x)
	policyQualifierId	x id-qt-cps	x id-qt-cps
	qualifier	x CPSuri	x CPSuri
	cPSuri	x (CPS URI)	x (CPS URI)
	userNotice	-	-
	policyInformation	(x)	(x)
	:	:	:
	:	:	:
	policyInformation	(x)	(x)
	BasicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints
	cA	TRUE	FALSE
	pathLenConstraint	2	-

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.15 (continued)**

ISO 15118-20 certificate profiles		Cross cross certificate	OCSP OCSP signer/re- sponder certificate
	CRLDistributionPoints (CRL)	(x) / nc id-ce-cRLDistributionPoints	-
	distributionPoint	x	-
	distributionPointName	(x) (see [V2G20-3038] and B.2.3.2.1)	-
	fullName	x (in GeneralNames format)	-
	generalName	x uniformResourceIdentifier [6]	-
	nameRelativeToCRLIssuer	-	-
	reasons	-	-
	cRLIssuer	(x) (see B.2.3.2.1)	-
	distributionPoint	-	-
	AuthorityInfoAccess	(x) / nc id-pe-authorityInfoAccess	-
	accessDescription (OCSP)	x	-
	accessMethod	x id-ad-ocsp	-
	accessLocation	x (location of the OCSP responder)	-
	generalName	x uniformResourceIdentifier [6]	-
	accessDescription	-	-
	SubjectInfoAccess	x / nc id-pe-subjectInfoAccess	-
	accessDescription (CrossCertIndication)	x	-
	accessMethod	x id-crossCertIndication (see [V2G20-2604])	-
	accessLocation	x	-
	generalName	x otherName [0]	-
	type-id	x id-utf8String (see [V2G20-3077])	-

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.15 (continued)

ISO 15118-20 certificate profiles		Cross cross certificate	OCSP OCSP signer/responder certificate
	value	x “ROOT CA CROSS” (Syntax: An alphanumeric string with a maximum length of 13 bytes as described here)	-
	accessDescription	-	-
Signature-Algorithm	AlgorithmIdentifier	x	x
	algorithm	x ecdsa-with-SHA512	x ecdsa-with-SHA512
	parameters	-	-
Signature Value		(Octet-String)	(Octet-String)
		(This cross certificate profile shall be applied for all cross certificates regardless of the certificate structure)	(This OCSP signer certificate profile shall be applied for all OCSP responder leaf certificates for all Sub-CAs and leafs that use OCSP regardless of the certificate structure)

NOTE 1 OID values for ‘ecdsa-with-SHA512’, ‘id-ecPublicKey’ and ‘secp521r1’ can be found in B.1.

Clause B.9.2

Replace entire text in this clause, and Table B.16 with:

Table B.16 outlines the cross certificate and OCSP signer/responder certificate based on curves as defined by [V2G20-2319].

Table B.16 — Cross certificate and OCSP signer/responder certificate based on curves as defined by [V2G20-2319]

ISO 15118-20 certificate profiles		Cross cross certificate	OCSP OCSP signer/responder certificate
	Version	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)
	SerialNumber	x	x
Signature	AlgorithmIdentifier	x	x
	algorithm	x id-Ed448	x id-Ed448
	parameters	-	-

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.16 (continued)**

ISO 15118-20 certificate profiles		Cross cross certificate	OCSP OCSP signer/re- sponder certificate
Issuer	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x
	Organization Unit (OU)	(x)	(x)
	Common Name (CN)	x	x
	Domain Component (DC)	(x)	(x)
Validity	Validity	x [up to issuer]	x [up to 1 year]
Subject	Country (C)	(x) (ISO 3166-1 alpha-2 code)	-
	Organization (O)	x	x
	Organization Unit (OU)	(x)	(x)
	Common Name (CN)	x	x
	Domain Component (DC)	(x)	(x)
SubjectPub- licKeyInfo	AlgorithmIdentifier	x	x
	algorithm	x id-Ed448	x id-Ed448
	parameters	-	-
	SubjectPublicKey	x (BIT STRING)	x (BIT STRING)
IssuerUniqueID		-	-
SubjectUniqueID		-	-
	AuthorityKeyIdentifier	x / nc id-ce-authorityKeyIdentifier	x / nc id-ce-authorityKeyIdentifier
	keyIdentifier	x (see [V2G20-1851])	x (see [V2G20-1851])
	authorityCertIssuer	-	-
	authorityCertSerialNumber	-	-
	SubjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier
	keyIdentifier	x (see [V2G20-1852])	x (see [V2G20-1852])
	KeyUsage	x / c	x / c
	digitalSignature	0/1	0/1

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.16 (continued)

ISO 15118-20 certificate profiles		Cross cross certificate	OCSP OCSP signer/re- sponder certificate
TbsCertificate	nonRepudiation (contentCommitment)	0/1	0/1
	keyEncipherment	0/1	0/1
	dataEncipherment	0	0
	keyAgreement	0/1	0
	keyCertSign	1	0
	cRLSign	0/1	0
	encipherOnly	0	0
	decipherOnly	0	0
	ExtendedKeyUsage	-	x / c id-ce-extKeyUsage
	keyPurposeId	-	x id-kp-OCSPSigning
	CertificatePolicies	(x) / nc	(x) / nc
	policyInformation	x	x
	certPolicyId	x (OID of the policy)	x (OID of the policy)
	policyQualifierInfo	(x)	(x)
	policyQualifierId	x id-qt-cps	x id-qt-cps
	qualifier	x CPSuri	x CPSuri
	cPSuri	x (CPS URI)	x (CPS URI)
	userNotice	-	-
Extensions	policyInformation	(x)	(x)
	:	:	:
	:	:	:
	policyInformation	(x)	(x)
	BasicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints
	cA	TRUE	FALSE
	pathLenConstraint	2	-
	CRLDistribution- Points (CRL)	(x) / nc id-ce-CRLDistribution- Points	-
	distributionPoint	x	-
	distributionPoint- Name	(x) (location of the CRL distributer. If not present, defaults to cRLIssuer)	-
	fullName	x (in GeneralNames format)	-

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**
Table B.16 (continued)

ISO 15118-20 certificate profiles		Cross cross certificate	OCSP OCSP signer/re- sponder certificate
	generalName	x uniformResourceIdentifier [6]	-
	nameRelativeToCRLIssuer	-	-
	reasons	(x) (revocation reasons covered by the CRL)	-
	cRLIssuer	(x) (authority that issues the CRL. If not present, defaults to Issuer name above)	-
	distributionPoint	x	-
	AuthorityInfoAccess	(x) / nc id-pe-authorityInfoAccess	-
	accessDescription (OCSP)	x	-
	accessMethod	x id-ad-ocsp	-
	accessLocation	x (location of the OCSP responder)	-
	generalName	x uniformResourceIdentifier [6]	-
	accessDescription	-	-
	SubjectInfoAccess	x / nc id-pe-subjectInfoAccess	-
	accessDescription (CrossCertIndication)	x	-
	accessMethod	x id-crossCertIndication (see [V2G20-2604])	-
	accessLocation	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 characters as described here)	-
	generalName	x otherName [0]	-
	type-id	x id-utf8String (see [V2G20-3077])	-

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.16 (continued)

ISO 15118-20 certificate profiles		Cross cross certificate	OCSP OCSP signer/responder certificate
	value	x "ROOT CA CROSS" (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	-
	accessDescription	-	-
Signature-Algorithm	AlgorithmIdentifier	x	x
	algorithm	x id-Ed448	x id-Ed448
	parameters	-	-
Signature Value		(Raw BIT STRING)	(Raw BIT STRING)
		(This cross certificate profile shall be applied for all cross certificates regardless of the certificate structure)	(This OCSP signer certificate profile shall be applied for all OCSP responder leaf certificates for all SubCAs and leafs that use OCSP regardless of the certificate structure)

Clause B.9.3

Replace entire text in this clause with:

As mentioned in Table B.15 and Table B.16, it is optional to include the 'certificatePolicies' extension in any of the cross certificates and OCSP signer/responder certificates. If the 'certificatePolicies' extension is included, it can be marked as non-critical so that, if allowed by the local policy, the relying party can ignore this extension if it cannot process it. This is done to improve the interoperability.

[V2G20-2601] Cross certificate shall contain either 'CRLDistributionPoints' extension or 'AuthorityInfoAccess' extension or both.

NOTE 1 Table B.15 and Table B.16 specify that both 'CRLDistributionPoints' and 'AuthorityInfoAccess' extensions are optional to indicate that either one of them can be included. [V2G20-2601] clarifies that including at least one of them is mandatory while including both is not mandatory.

NOTE 2 [V2G20-2601] does not specify which one of these extensions can be included. It is left up to the CA to decide which certificate revocation method works best for it. In some cases CRLs will work better as they allow the relying party to download the entire CRL once and have it available for local checking of revocation status of the next cross certificate without a need for a live connection to the CRL server while in other cases OCSP will provide better results as it provides current revocation status and requires less storage and searching on part of the relying party.

[V2G20-2602] If cross certificate contains both 'CRLDistributionPoints' and 'AuthorityInfoAccess' extensions, the relying party may process just one or both as per the local policy of the relying party. However, the relying party shall process at least one of these extensions.

NOTE 3 Table B.15 and Table B.16 specify that both 'CRLDistributionPoints' and 'AuthorityInfoAccess' extensions are optional to indicate that at least one of them is included. [V2G20-2602] clarifies that if the issuer desires to include both, it is up to the relying party to decide which one to process. [V2G20-2602] also ensures that the relying party will process at least one.

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

[V2G20-3076] If cross certificate contains only one of ‘CRLDistributionPoints’ and ‘AuthorityInfoAccess’ extensions, the relying party shall process the extension that is present.

NOTE 4 Table B.15 and Table B.16 specify that both ‘CRLDistributionPoints’ and ‘AuthorityInfoAccess’ extensions are optional and [V2G20-2601] specifies that it is mandatory to include at least one of them. [V2G20-2591] ensures that, if only one of them is included, the relying party will process that one.

[V2G20-2603] The cross certificate extensions in Table B.15 and Table B.16 shall use the definition of ‘SubjectInfoAccess’ as defined in IETF RFC 5280, 4.2.2.2, to indicate that the particular certificate is cross certified. As mentioned in IETF RFC 5280, the field ‘accessMethod’ indicates the type of information and the field ‘accessLocation’ indicates either the information itself or a storage location for the information.

NOTE 5 IETF RFC 5280 has been updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399. These updates are considered to be included in this document.

‘SubjectInfoAccess’ is defined as a non-critical extension. This document does not require the relying parties relying on and/or processing the cross certificate to process this extension. It is left to the local policy of the relying party whether it needs to process this extension.

[V2G20-2604] The issuer of the certificate shall describe the information with one additional access method for ‘accessMethod’. Here are the definitions in ASN.1 notation:

```
ISO15118-Extensions { iso(1) standard(0) 15118 part20(20) extensions(0) }
DEFINITIONS :=
BEGIN
  id-15118-20-ad          OBJECT IDENTIFIER ::= { iso(1) standard(0) 15118 part20(20)
                                                extensions(0) }

  -- Indication that this certificate is a cross-certificate
  id-crossCertIndication OBJECT IDENTIFIER ::= { id-15118-20-ad
                                                crossCertIndication (6) }

END
```

NOTE 6 Refer to ITU-T X.680 for details of ASN.1 notation.

[V2G20-3077] The issuer of the certificate shall describe the information with one additional other name for type field in ‘otherName’. Here are the definitions in ASN.1 notation:

```
ISO15118-Extensions { iso(1) standard(0) 15118 part20(20) extensions(0) }
DEFINITIONS :=
BEGIN
  id-15118-20-ad          OBJECT IDENTIFIER ::= { iso(1) standard(0) 15118
                                                part20(20)                                         extensions(0) }

  -- an UTF8 string
  id-utf8String            OBJECT IDENTIFIER ::= { id-15118-20-ad utf8String(7) }
```

NOTE 7 Refer to ITU-T X.680 for details of ASN.1 notation.

Refer to H.1.5 and its subclauses for further details on cross-signing.

[V2G20-3078] The OCSP responder certificate shall contain the public key corresponding to the private key used to sign the OCSP response.

Clause B.10.1

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Replace Table B.17 with this table:

Table B.17 — Certificates for a private environment based on curves as defined by [V2G20-2674]

ISO 15118-20 certificate profiles		Private SECC/private environment			
		PE private root CA Root	PE Sub-CA 1 Sub (optional)	PE Sub-CA 2 Sub (optional)	PE Cert Leaf
Version	2 (“2” indicates X.509v3)	2 (“2” indicates X.509v3)	2 (“2” indicates X.509v3)	2 (“2” indicates X.509v3)	2 (“2” indicates X.509v3)
	x	x	x	x	x
Signature	AlgorithmIdentifier	x	x	x	x
	algorithm	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512
	parameters	-	-	-	-
Issuer	Country (C)	(x) (ISO 3166-1 alpha-2 code)			
	Organization (O)	x	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)	(x)
	Common Name (CN)	x	x	x	x
	Domain Component (DC)	(x)	(x)	(x)	(x)
Validity	Validity	x [40 years]	x [up to PE]	x [up to PE]	x [2-20 years]
Subject	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	x (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)	(x)
	Common Name (CN)	x	x	x	x PEID (see [V2G20-3079])
	Domain Component (DC)	(x)	(x)	(x)	(x) & “PE”
Subject-PublicKey-Info	AlgorithmIdentifier	x	x	x	x
	algorithm	x id-ecPublicKey	x id-ecPublicKey	x id-ecPublicKey	x id-ecPublicKey
	parameters (ECParameters)	x	x	x	x
	namedCurve	x secp521r1	x secp521r1	x secp521r1	x secp521r1
	SubjectPublicKey	x (BIT STRING)	x (BIT STRING)	x (BIT STRING)	x (BIT STRING)
IssuerUniqueID		-	-	-	-

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.17 (continued)**

ISO 15118-20 certificate profiles		Private SECC/private environment			
		PE private root CA Root	PE Sub-CA 1 Sub (optional)	PE Sub-CA 2 Sub (optional)	PE Cert Leaf
TbsCertificate	SubjectUniqueID	-	-	-	-
	AuthorityKeyIdentifier	-	x / nc id-ce-authorityKeyIdentifier	x / nc id-ce-authorityKeyIdentifier	x / nc id-ce-authorityKeyIdentifier
	keyIdentifier	-	x (see [V2G20-1851])	x (see [V2G20-1851])	x (see [V2G20-1851])
	authorityCertIssuer	-	-	-	-
	authorityCertSerialNumber	-	-	-	-
	SubjectKeyIdentifier	x / nc id-ce-subject-KeyIdentifier	x / nc id-ce-subject-KeyIdentifier	x / nc id-ce-subject-KeyIdentifier	x / nc id-ce-subject-KeyIdentifier
	keyIdentifier	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])
	KeyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage
	digitalSignature	0/1	0/1	0/1	1
	nonRepudiation (contentCommitment)	0/1	0/1	0/1	0/1
	keyEncipherment	0/1	0/1	0/1	0/1
	dataEncipherment	0	0	0	0
	keyAgreement	0/1	0/1	0/1	0/1
	keyCertSign	1	1	1	0
	cRLSign	0	0	0	0
	encipherOnly	0	0	0	0
	decipherOnly	0	0	0	0
	ExtendedKeyUsage	-	-	-	x / c id-ce-extKeyUsage
	keyPurposeId	-	-	-	x id-kp-server-Auth
	CertificatePolicies	-	(x) / nc	(x) / nc	(x) / nc
	policyInformation	-	x	x	x
	certPolicyId	-	x (OID of the policy)	x (OID of the policy)	x (OID of the policy)
	policyQualifierInfo	-	(x)	(x)	(x)
	policyQualifierId	-	x id-qt-cps	x id-qt-cps	x id-qt-cps

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.17 (continued)

ISO 15118-20 certificate profiles		Private SECC/private environment			
		PE private root CA Root	PE Sub-CA 1 Sub (optional)	PE Sub-CA 2 Sub (optional)	PE Cert Leaf
Extensions	qualifier	-	x CPSuri	x CPSuri	x CPSuri
	cPSuri	-	x (CPS URI)	x (CPS URI)	x (CPS URI)
	userNotice	-	-	-	-
	policyInformation	-	(x)	(x)	(x)
	:	-	:	:	:
	:	-	:	:	:
	policyInformation	-	(x)	(x)	(x)
	BasicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints
	cA	TRUE	TRUE	TRUE	FALSE
	pathLenConstraint	-	1	0	-
	AuthorityInfoAccess	-	(x) / nc id-pe-authority-InfoAccess	(x) / nc id-pe-authority-InfoAccess	(x) / nc id-pe-authority-InfoAccess
	accessDescription (OCSP)	-	x	x	x
	accessMethod	-	x id-ad-ocsp	x id-ad-ocsp	x id-ad-ocsp
	accessLocation	-	x (location of the OCSP responder)	x (location of the OCSP responder)	x (location of the OCSP responder)
	generalName	-	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]
	accessDescription	-	-	-	-
	SubjectInfoAccess	-	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	-
	accessDescription (CrossCertIndication)	-	x	x	-
	accessMethod	-	x id-crossCertIndication (see [V2G20-2604])	x id-crossCertIndication (see [V2G20-2604])	-
	accessLocation	-	x	x	-

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**
Table B.17 (continued)

ISO 15118-20 certificate profiles		Private SECC/private environment			
		PE private root CA Root	PE Sub-CA 1 Sub (optional)	PE Sub-CA 2 Sub (optional)	PE Cert Leaf
		generalName	-	x otherName [0]	x otherName [0]
		type-id	-	x id-utf8String (see [V2G20-3077])	x id-utf8String (see [V2G20-3077])
		value	-	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)
		accessDescription	-	-	-
Signature-Algorithm	AlgorithmIdentifier	x	x	x	x
	algorithm	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512	x ecdsa-with-SHA512
	parameters	-	-	-	-
Signature Value		(Octet-String)	(Octet-String)	(Octet-String)	(Octet-String)

Delete NOTE 1 below Table B.17 and renumber NOTE 2.

Clause B.10.2

Replace Table B.18 with this table:

Table B.18 — Certificates for a private environment based on curves as defined by [V2G20-2319]

ISO 15118-20 certificate profiles		Private SECC/private environment			
		PE private root CA Root	PE Sub-CA 1 Sub (optional)	PE Sub-CA 2 Sub (optional)	PE Cert Leaf
	Version	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)	2 ("2" indicates X.509v3)
	SerialNumber	x	x	x	x
	Signature	x AlgorithmIdentifier	x	x	x
		x algorithm	x id-Ed448	x id-Ed448	x id-Ed448
		parameters	-	-	-

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**
Table B.18 (continued)

ISO 15118-20 certificate profiles		Private SECC/private environment			
		PE private root CA Root	PE Sub-CA 1 Sub (optional)	PE Sub-CA 2 Sub (optional)	PE Cert Leaf
Issuer	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)	(x)
	Common Name (CN)	x	x	x	x
	Domain Component (DC)	(x)	(x)	(x)	(x)
Validity	Validity	x [40 years]	x [up to PE]	x [up to PE]	x [2-20 years]
Subject	Country (C)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	(x) (ISO 3166-1 alpha-2 code)	x (ISO 3166-1 alpha-2 code)
	Organization (O)	x	x	x	x
	Organization Unit (OU)	(x)	(x)	(x)	(x)
	Common Name (CN)	x	x	x	x PEID (see [V2G20-3079])
	Domain Component (DC)	(x)	(x)	(x)	(x) & "PE"
Subject-PublicKey-Info	AlgorithmIdentifier	x	x	x	x
	algorithm	x id-Ed448	x id-Ed448	x id-Ed448	x id-Ed448
	parameters	-	-	-	-
	SubjectPublicKey	x (BIT STRING)	x (BIT STRING)	x (BIT STRING)	x (BIT STRING)
IssuerUniqueID		-	-	-	-
SubjectUniqueID		-	-	-	-
	AuthorityKeyIdentifier	-	x / nc id-ce-authorityKeyIdentifier	x / nc id-ce-authorityKeyIdentifier	x / nc id-ce-authorityKeyIdentifier
	keyIdentifier	-	x (see [V2G20-1851])	x (see [V2G20-1851])	x (see [V2G20-1851])
	authorityCertIssuer	-	-	-	-
	authorityCertSerialNumber	-	-	-	-
	SubjectKeyIdentifier	x / nc id-ce-subject-KeyIdentifier	x / nc id-ce-subject-KeyIdentifier	x / nc id-ce-subject-KeyIdentifier	x / nc id-ce-subject-KeyIdentifier
	keyIdentifier	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])	x (see [V2G20-1852])

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**
Table B.18 (continued)

ISO 15118-20 certificate profiles		Private SECC/private environment			
		PE private root CA Root	PE Sub-CA 1 Sub (optional)	PE Sub-CA 2 Sub (optional)	PE Cert Leaf
TbsCertificate	KeyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage	x / c id-ce-keyUsage
	digitalSignature	0/1	0/1	0/1	1
	nonRepudiation (contentCommitment)	0/1	0/1	0/1	0/1
	keyEncipherment	0/1	0/1	0/1	0/1
	dataEncipherment	0	0	0	0
	keyAgreement	0/1	0/1	0/1	0/1
	keyCertSign	1	1	1	0
	cRLSign	0	0	0	0
	encipherOnly	0	0	0	0
	decipherOnly	0	0	0	0
	ExtendedKeyUsage	-	-	-	x / c id-ce-extKeyUsage
	keyPurposeId	-	-	-	x id-kp-serverAuth
	CertificatePolicies	-	(x) / nc	(x) / nc	(x) / nc
	policyInformation	-	x	x	x
	certPolicyId	-	x (OID of the policy)	x (OID of the policy)	x (OID of the policy)
	policyQualifierInfo	-	(x)	(x)	(x)
	policyQualifierId	-	x id-qt-cps	x id-qt-cps	x id-qt-cps
	qualifier	-	x CPSuri	x CPSuri	x CPSuri
	cPSuri	-	x (CPS URI)	x (CPS URI)	x (CPS URI)
Extensions	userNotice	-	-	-	-
	policyInformation	-	(x)	(x)	(x)
	:	-	:	:	:
	:	-	:	:	:
	policyInformation	-	(x)	(x)	(x)
	BasicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints	x / c id-ce-basicConstraints
	cA	TRUE	TRUE	TRUE	FALSE
pathLenConstraint	-	1	0	-	-
	AuthorityInfoAccess (OCSP)	-	(x) / nc id-pe-authority-InfoAccess	(x) / nc id-pe-authority-InfoAccess	(x) / nc id-pe-authority-InfoAccess

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table B.18 (continued)

ISO 15118-20 certificate profiles		Private SECC/private environment			
		PE private root CA Root	PE Sub-CA 1 Sub (optional)	PE Sub-CA 2 Sub (optional)	PE Cert Leaf
Signature-Algorithm	accessDescription (OCSP)	-	x	x	x
	accessMethod	-	x id-ad-ocsp	x id-ad-ocsp	x id-ad-ocsp
	accessLocation	-	x (location of the OCSP responder)	x (location of the OCSP responder)	x (location of the OCSP responder)
	generalName	-	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]	x uniformResourceIdentifier [6]
	accessDescription	-	-	-	-
	SubjectInfoAccess	-	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	(x) / nc id-pe-subjectInfoAccess (see [V2G20-3046], [V2G20-3047] & [V2G20-3048])	-
	accessDescription (CrossCertIndication)	-	x	x	-
	accessMethod	-	x id-crossCertIndication (see [V2G20-2604])	x id-crossCertIndication (see [V2G20-2604])	-
	accessLocation	-	x	x	-
	generalName	-	x otherName [0]	x otherName [0]	-
	type-id	-	x id-utf8String (see [V2G20-3077])	x id-utf8String (see [V2G20-3077])	-
	value	-	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	x “CROSS” (Syntax: An alphanumeric string with a maximum length of 5 bytes as described here)	-
	accessDescription	-	-	-	-
	AlgorithmIdentifier	x	x	x	x
	algorithm	x id-Ed448	x id-Ed448	x id-Ed448	x id-Ed448
	parameters	-	-	-	-

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Table B.18 (continued)**

ISO 15118-20 certificate profiles	Private SECC/private environment			
	PE private root CA Root	PE Sub-CA 1 Sub (optional)	PE Sub-CA 2 Sub (optional)	PE Cert Leaf
Signature Value	(Raw BIT STRING)	(Raw BIT STRING)	(Raw BIT STRING)	(Raw BIT STRING)

Clause B.10.3

Replace entire text in this clause with:

As mentioned in Table B.17 and Table B.18, it is optional to include the ‘certificatePolicies’ extension in any of the PE Certificates. If the ‘certificatePolicies’ extension is included, it can be marked as non-critical so that, if allowed by the local policy, the relying party can ignore this extension if it cannot process it. This is done to improve the interoperability.

[V2G20-3079] PEID shall be an alpha-numeric string with maximum length of 64 characters that can be used to uniquely identify a Private SECC in a particular private environment.

NOTE 1 Uniqueness of PEID is only required between Private SECCs in a single private environment. Uniqueness of PEID is not required between Private SECCs in different/distinct private environments. Uniqueness of subject name is required between Private SECCs in different/distinct private environments.

[V2G20-3080] Subject field of the PE Certificate shall contain Domain Component ending with “PE”.

[V2G20-3081] The CA, at its discretion, may include any other necessary information in the Domain Component RDN of the Subject field of the PE Certificate without violating **[V2G20-3080]**.

[V2G20-2605] In case the Private SECC supports only EIM, PE Sub-CA1 Certificate, PE Sub-CA2 Certificate and PE Certificate may contain either ‘CRLDistributionPoints’ extension or ‘AuthorityInfoAccess’ extension or both.

NOTE 2 A Private SECC in EIM only mode is not required to support ‘CRLDistributionPoints’ and/or ‘AuthorityInfoAccess’ extensions.

[V2G20-2715] In case the Private SECC supports PnC, PE Sub-CA1 Certificate, PE Sub-CA2 Certificate and PE Certificate shall contain either ‘CRLDistributionPoints’ or ‘AuthorityInfoAccess’ extension or both.

NOTE 3 Table B.17 and Table B.18 specify that both ‘CRLDistributionPoints’ and ‘AuthorityInfoAccess’ extensions are optional to indicate that either of them can be included. If the SECC intends to provide PnC as an authorization mechanism, **[V2G20-2715]** clarifies that including at least one of them is mandatory while including both of them is not mandatory.

NOTE 4 **[V2G20-2715]** does not specify which one of these extensions can be included. It is left up to the CA to decide which certificate revocation method works best for it. In some cases CRLs will work better as they allow the relying party to download the entire CRL once and have it available for local checking of revocation status of the next PE certificate without a need for a live connection to the CRL server while in other cases OCSP will provide better results as it provides current revocation status and requires less storage and searching on part of the relying party.

[V2G20-2606] If PE Sub-CA1 Certificate or PE Sub-CA2 Certificate or PE Certificate contains both ‘CRLDistributionPoints’ and ‘AuthorityInfoAccess’ extensions, the relying party may process just one or both as per the local policy of the relying party. However, if the relying party plans to use PnC in the PE, the relying party shall process at least one of these extensions.

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

NOTE 5 Table B.17 and Table B.18 specify that both ‘CRLDistributionPoints’ and ‘AuthorityInfoAccess’ extensions are optional to indicate that at least one of them is included. [V2G20-2606] clarifies that if the issuer desires to include both, it is up to the relying party to decide which one to process. [V2G20-2606] also ensures that the relying party will process at least one.

[V2G20-3082] If PE Sub-CA1 Certificate or PE Sub-CA2 Certificate or PE Certificate contains only one of ‘CRLDistributionPoints’ and ‘AuthorityInfoAccess’ extensions and if the relying party plans to use PnC in the PE, the relying party shall process the extension that is present.

NOTE 6 Table B.17 and Table B.18 specify that both ‘CRLDistributionPoints’ and ‘AuthorityInfoAccess’ extensions are optional and [V2G20-2715] specifies that it is mandatory to include at least one of them if the Private SECC wants to provide PnC for authorization. [V2G20-2591] ensures that if only one of them is included and the relying party plans to use PnC, the relying party will process that one.

Refer to H.2 and its subclauses for further details on PE.

Refer to H.1.5 and its subclauses for further details on cross-signing.

Clause C.1.1

Replace requirement [V2G20-2126] with the following requirement:

[V2G20-3083] The maximum length of EMAID shall be 64 characters.

Clause C.2.1

Replace requirement [V2G20-2079] with the following requirement:

[V2G20-3084] PCID shall be an alphanumeric string with a length of minimum 18 and maximum 64 characters (i.e. A..Z, a..z, 0..9), including a check digit at the end.

Replace the following text in requirement [V2G20-2080]

<Check Digit> = *1 (ALPHA / DIGIT)

with this text:

<Check Digit> = 1 (ALPHA / DIGIT)

Clause C.3.1

Replace requirement [V2G20-2127] with the following requirement:

[V2G20-3085] SECCID shall be an alphanumeric string with a length of minimum 39 and maximum 64 characters (i.e. A..Z, a..z, 0..9), including a check digit at the end.

Replace the following text in requirement [V2G20-2083]

<Check Digit> = *1 (ALPHA / DIGIT)

with this text:

<Check Digit> = 1 (ALPHA / DIGIT)

Clause C.4.1

Replace requirement [V2G20-2088] with the following requirement:

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

[V2G20-3086] The maximum length of EVSEID shall be 64 characters.

Clause C.5.1

Replace requirement [V2G20-2089] with the following requirement:

[V2G20-3087] EVCCID shall be an alphanumeric string with a length of minimum 20 and maximum 64 characters (i.e. A..Z, a..z, 0..9), including a check digit at the end.

Replace the following text in requirement [V2G20-2093]

<Check Digit> = *1 (ALPHA / DIGIT)

with this text:

<Check Digit> = 1 (ALPHA / DIGIT)

Clause H.1.1

Replace reference in last sentence of last paragraph:

Finally, a visual overview of the resulting certificate structure and usage is given (refer to Annex H.1.6).

Clause H.1.5

Replace last paragraph in H.1.5 (above original clause H.1.5.1) with the following new subclauses H.1.5.1, H.1.5.1.1, H.1.5.1.2, H.1.5.1.3, H.1.5.1.4, H.1.5.1.5:

H.1.5.1 Certificate level and certificate structure

This document neither mandates cross-certification nor prevents it. Cross certification is possible at Root CA or at Sub-CA levels. This document simply opens the door for the possibility of cross-certification in case the industry chooses to do so. To that end, this document allows a certificate chain to contain up to 4 certificates (one leaf, two Sub-CAs, and one cross-certificate) when a cross certificate is used. IETF RFC 6712 provides details of a protocol that can be used to generate cross-certificates. This document, however, does not define protocol used for cross-certificate generation. Reference to IETF RFC 6712 is simply provided as a commonly used example.

Cross-certification can only occur between CAs. An end-entity cannot be cross certified. Keeping this and [V2G20-1005] and [V2G20-1002] in mind while meeting the path length constraints defined by the profiles specified in Annex B, following cross certification restrictions exist:

- A Root-CA is not limited in which CAs it can cross certify. As per the local policy of the Root-CA, a Root-CA can cross certify another Root-CA or a Sub-CA1 or a Sub-CA2.
- A Sub-CA1 can only cross certify Sub-CA2. A Sub-CA1 cannot cross certify another Sub-CA1 or a Root-CA as that would violate the path length constraints defined by the profiles specified in Annex B.
- A Sub-CA2 cannot issue cross certificates as that would violate either the chain length constraints specified by [V2G20-1005] or the path length constraints defined by the profiles specified in Annex B.

All cross certified Sub-CAs will have more than one (1) active certificates assigned to them. The main certificate will be from the chain under which the Sub-CA was established. Other certificate(s) will be from the CA(s) (Root-CA or Sub-CA1, as the case may be) cross certifying the Sub-CA. These 'other' certificates for the Sub-CA will meet **[V2G20-3046]** and contain an indication that they are cross certificates.

All Sub-CA certificates, regardless of whether they are cross certified or not, will meet the appropriate Sub-CA profiles as specified in B.4, B.5, B.6, B.7, B.8 and B.10 (and their subclauses) in Annex B.

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

However, cross-certification at the Root-CA level will be slightly different. Cross-certification between 2 Root-CAs will generate a cross certificate which will match the cross certificate profile as specified in B.9 (and its subclauses) in Annex B.

These constraints lead to many possible certificate structures with cross-certification. Following subclauses depict examples of a few of those. Most examples are provided for unilateral cross-certification, though mutual cross-certification and multilateral cross-certification is also possible. These examples do not cover all permutations and combinations possible within the constraints specified.

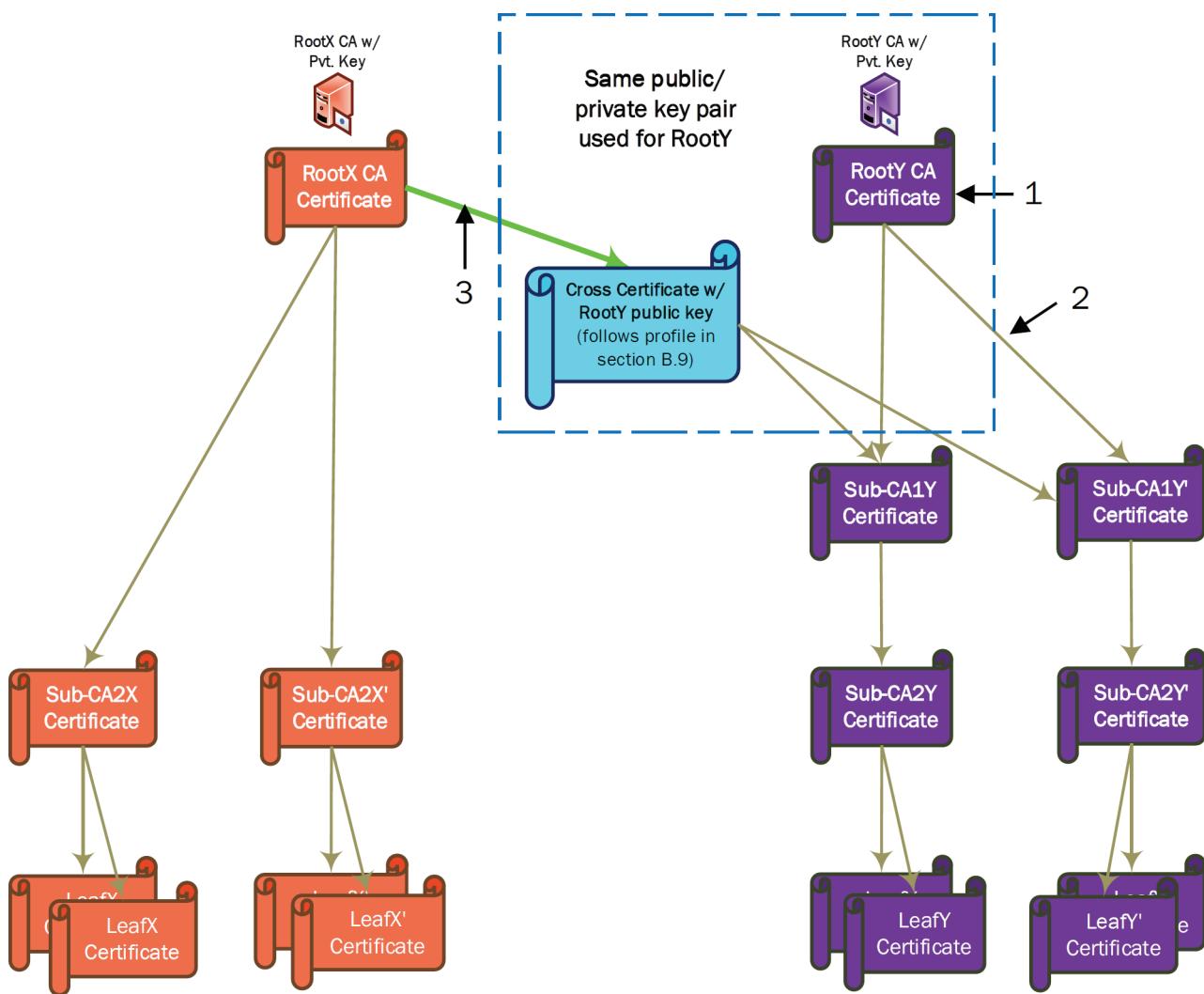
Each example certificate structure will have different possible certificate chains that will need to be stored in the end entity. H.1.5.3.2 talks about certain risks associated with this approach.

Cross certification for contract certificates leads to additional complexity in installation, management, and handling of contract certificates, including usage of these certificates. For example, the EVCC can only send one contract certificate chain at a time with AuthorizationReq but with cross certification, EVCC might have multiple certificate chains for the same contract certificate. Providing each one of them, one at a time, may lead to increased time for Authorization.

This version of this standard does not account for cross certification for contract certificates.

H.1.5.1.1 Cross certification at Root-CA level

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

**Key**

- 1 certificate
- 2 direct certification
- 3 cross certification

Figure H.1 — Example of cross certification at Root CA level

This leads to the following certificate chains for LeafY:

- Sub-CA1Y certificate – Sub-CA2Y certificate – LeafY certificate
- Cross certificate (RootX->RootY) – Sub-CA1Y certificate – Sub-CA2Y certificate – LeafY certificate

The cross certificate leads to a certificate chain length of 4 which meets [V2G20-1005] while remaining within the path length constraints as defined by Annex B.

Per [V2G20-911], Sub-CA1 is optional. If Sub-CA1 is not used, it leads to the certificate chains as follows (example certificate structure not shown):

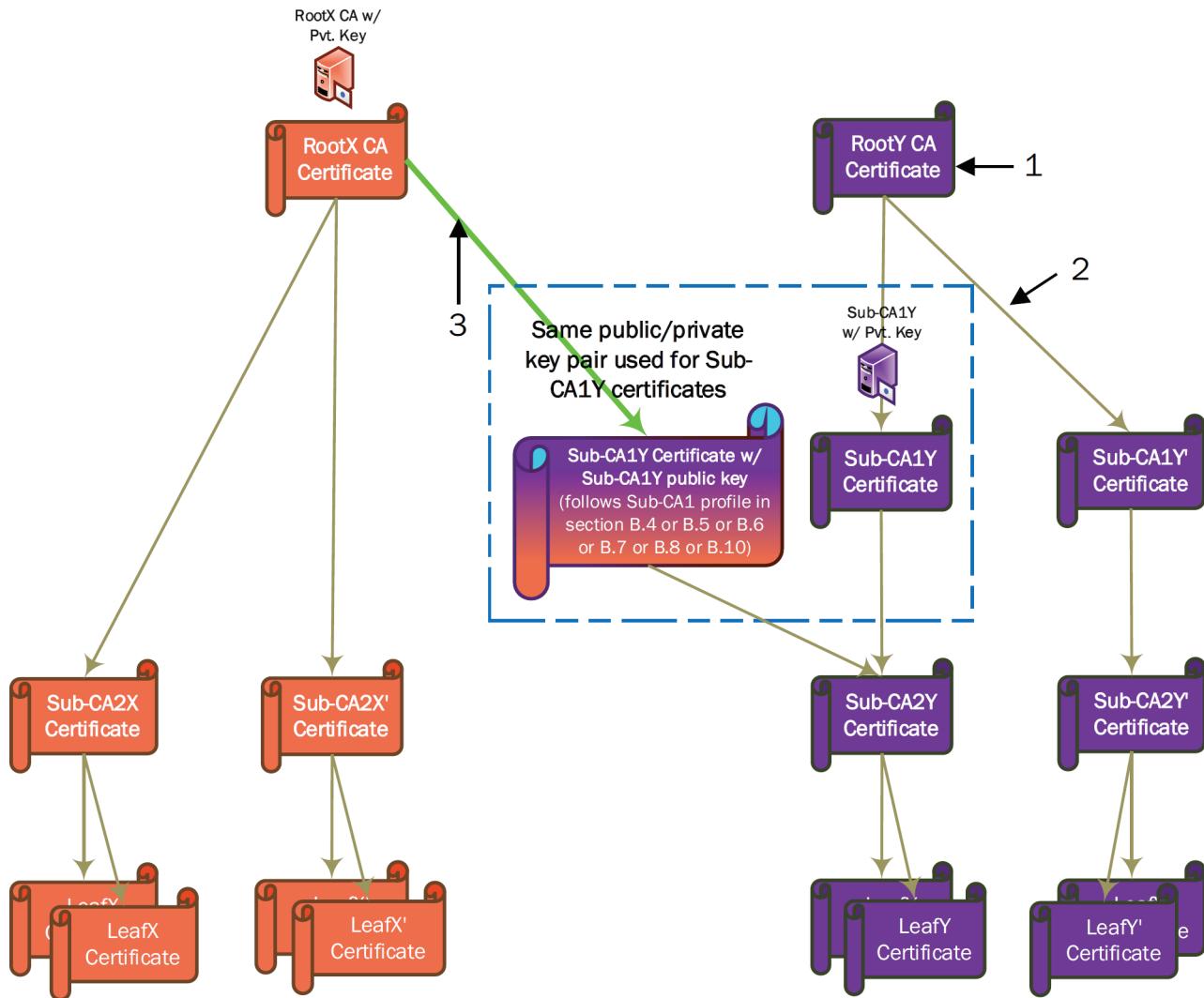
- Sub-CA2Y certificate – LeafY certificate
- Cross certificate (RootX->RootY) – Sub-CA2Y certificate – LeafY certificate

In this case, the cross certificate leads to a certificate chain length of 3 which still meets [V2G20-1005] while remaining within the path length constraints as defined by Annex B.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

As shown in Figure H.1, the certificate chains for both LeafY certificates and LeafY' certificates can be verified using either RootX or RootY.

H.1.5.1.2 Root-CA cross certifying Sub-CA1



Key

- 1 certificate
- 2 direct certification
- 3 cross certification

Figure H.2 — Example of Root-CA cross certifying Sub-CA1

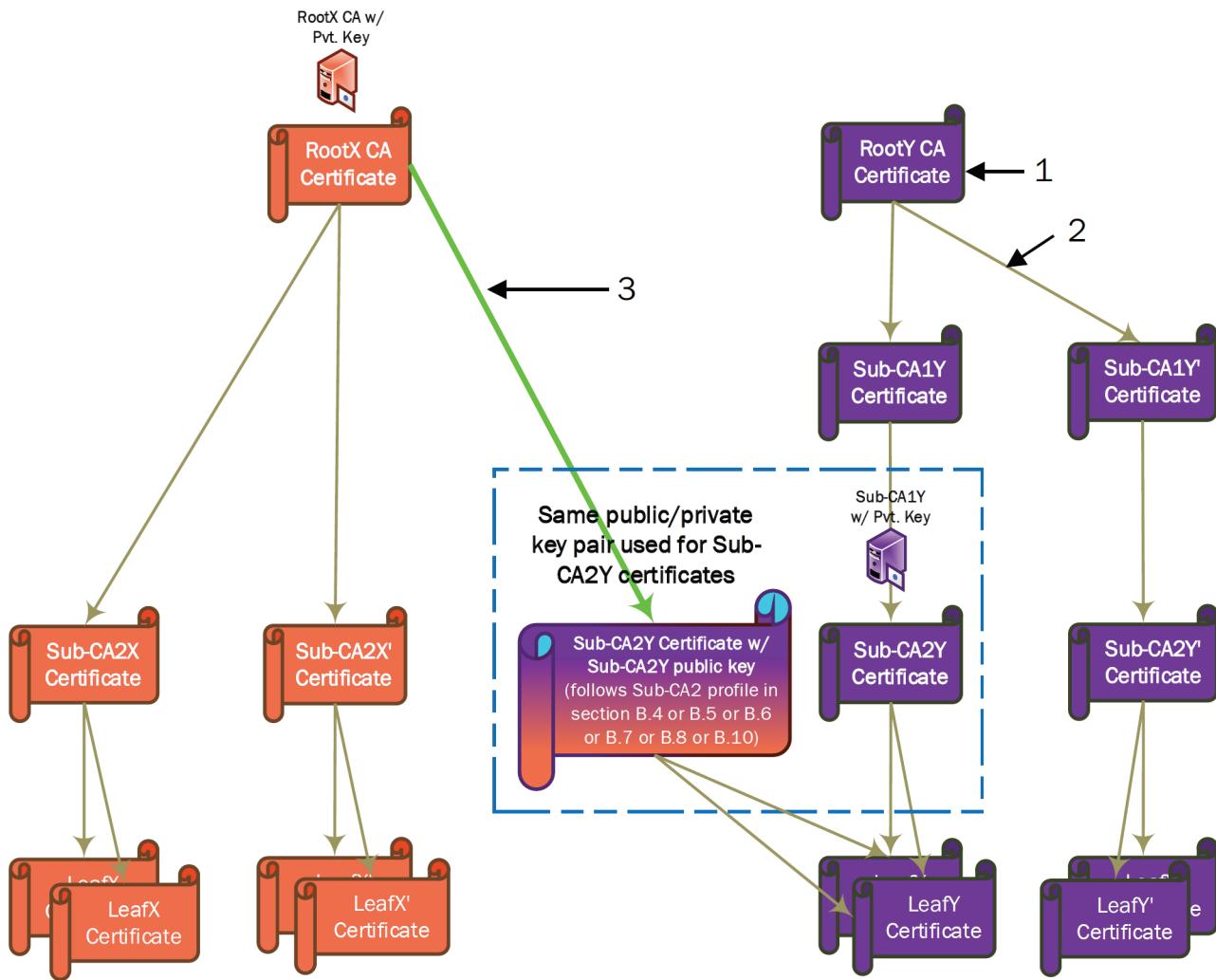
This leads to the following certificate chains for LeafY:

- Sub-CA1Y certificate – Sub-CA2Y certificate – LeafY certificate
- Sub-CA1Y certificate cross certified by RootX – Sub-CA2Y certificate – LeafY certificate

In this example, cross certification does not change the certificate chain length which stays at 3 and meets [V2G20-1005] while remaining within the path length constraints as defined by Annex B.

As shown in Figure H.2, the certificate chain for LeafY certificates can be verified using either RootX or RootY. However, the same figure also shows that the certificate chain for LeafY' certificates can only be verified using RootY. In this example, RootX cannot be used to verify certificate chain for LeafY' certificates.

H.1.5.1.3 Root-CA cross certifying Sub-CA2

**Key**

- 1 certificate
- 2 direct certification
- 3 cross certification

Figure H.3 — Example of Root-CA cross certifying Sub-CA2

This leads to the following certificate chains for LeafY:

- Sub-CA1Y certificate – Sub-CA2Y certificate – LeafY certificate
- Sub-CA2Y certificate cross certified by RootX – LeafY certificate

In this example, cross certification reduces the certificate chain length to 2 which meets [V2G20-1005] while remaining within the path length constraints as defined by Annex B.

Per [V2G20-911], Sub-CA1 is optional. If Sub-CA1 is not used, it leads to the certificate chains as follows:

- Sub-CA2Y certificate – LeafY certificate
- Sub-CA2Y certificate cross certified by RootX – LeafY certificate

In this case, cross certification does not change the certificate chain length which stays at 2 and meets [V2G20-1005] while remaining within the path length constraints as defined by Annex B.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

As shown in Figure H.3, the certificate chain for LeafY certificates can be verified using either RootX or RootY. However, the same figure also shows that the certificate chain for LeafY' certificates can only be verified using RootY. In this example, RootX cannot be used to verify certificate chain for LeafY' certificates.

H.1.5.1.4 Sub-CA1 cross certifying Sub-CA2

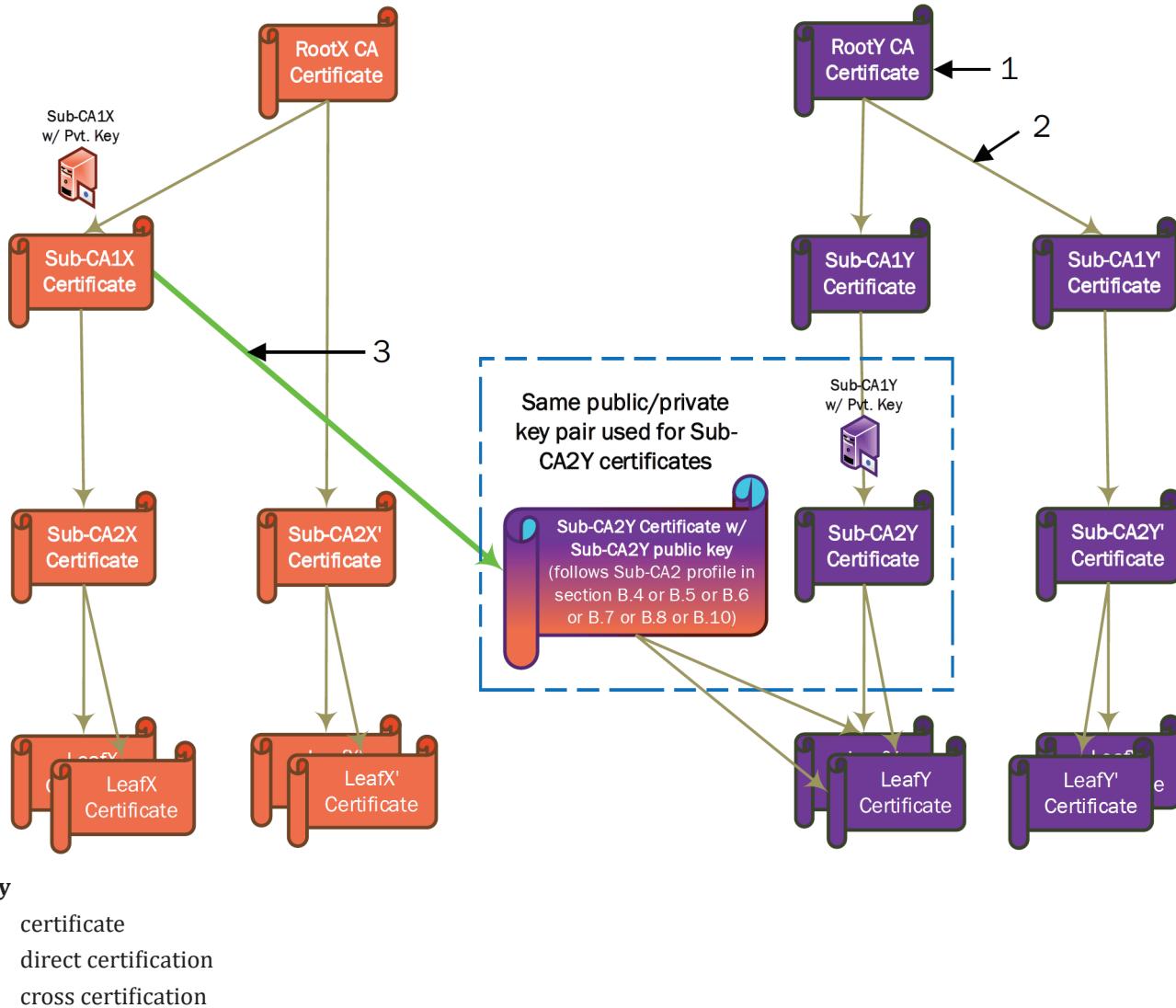


Figure H.4 — Example of Sub-CA1 cross certifying Sub-CA2

This leads to the following certificate chains for LeafY:

- Sub-CA1Y certificate – Sub-CA2Y certificate – LeafY certificate
- Sub-CA1X certificate – Sub-CA2Y certificate cross certified by Sub-CA1X – LeafY certificate

In this example, cross certification does not change the certificate chain length which stays at 3 and meets [V2G20-1005] while remaining within the path length constraints as defined by Annex B.

Per [V2G20-911], Sub-CA1 is optional. If Sub-CA1 is not used, it leads to the certificate chains as follows:

- Sub-CA2Y certificate – LeafY certificate
- Sub-CA1X certificate – Sub-CA2Y certificate cross certified by Sub-CA1X – LeafY certificate

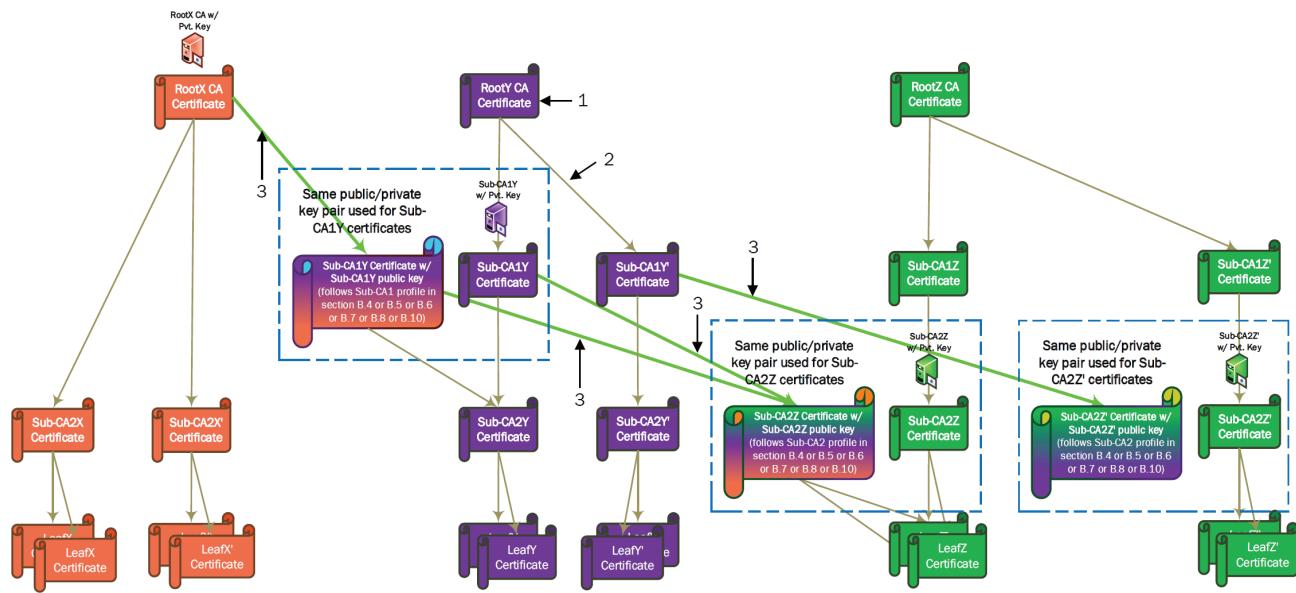
In this case, cross certification increases the certificate chain length to 3 and meets [V2G20-1005] while still remaining within the path length constraints as defined by Annex B.

E DIN EN ISO 15118-20/A1:2025-02

ISO 15118-20:2022/DAM 1:2024(en)

As shown in Figure H.4, the certificate chain for LeafY certificates can be verified using either RootX or RootY. However, the same figure also shows that the certificate chain for LeafY' certificates can only be verified using RootY. In this example, RootX cannot be used to verify certificate chain for LeafY' certificates.

H.1.5.1.5 Multilateral cross certification



Key

- 1 certificate
- 2 direct certification
- 3 cross certification

Figure H.5 — Example of Multilateral cross certification

This leads to the following certificate chains for LeafY:

- Sub-CA1Y certificate – Sub-CA2Y certificate – LeafY certificate
- Sub-CA1Y certificate cross certified by RootX – Sub-CA2Y certificate – LeafY certificate

In this example, cross certification does not change the certificate chain length which stays at 3 and meets [V2G20-1005] while remaining within the path length constraints as defined by Annex B.

As shown in Figure H.5, the certificate chain for LeafY certificates can be verified using either RootX or RootY. However, the same figure also shows that the certificate chain for LeafY' certificates can only be verified using RootY. In this example, RootX cannot be used to verify certificate chain for LeafY' certificates.

The cases for LeafZ and Leaf Z' are more interesting. Following are the certificate chains for LeafZ:

- Sub-CA1Z certificate – Sub-CA2Z certificate – LeafZ certificate
- Sub-CA1Y certificate – Sub-CA2Z certificate cross certified by Sub-CA1Y – LeafZ certificate
- Sub-CA1Y certificate cross certified by RootX – Sub-CA2Z certificate cross certified by Sub-CA1Y – LeafZ certificate

In this example, cross certification does not change the certificate chain length which stays at 3 and meets [V2G20-1005] while remaining within the path length constraints as defined by Annex B.

As shown in Figure H.5, this allows the certificate chain for LeafZ certificates to be verified using either RootX or RootY or Root Z.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Following are the certificate chains for LeafZ':

- Sub-CA1Z' certificate – Sub-CA2Z' certificate – LeafZ' certificate
- Sub-CA1Y' certificate – Sub-CA2Z' certificate cross certified by Sub-CA1Y' – LeafZ' certificate

Similar to above, in this example, cross certification does not change the certificate chain length which stays at 3 and meets [V2G20-1005] while remaining within the path length constraints as defined by Annex B.

However, unlike LeafZ, LeafZ' certificate chain can only be verified using either RootY or Root Z. RootX cannot be used to verify the certificate chains for LeafZ' certificates.

Clause H.1.5

Insert new clause H.1.5.2 above original H.1.5.1 and renumber the original clauses H.1.5.1 (Mutual cross certification) and H.1.5.2 (Unilateral cross certification) as subclauses:

H.1.5.2 Types of cross certification

H.1.5.2.1 Mutual cross certification

H.1.5.2.2 Unilateral cross certification

Insert new clause H.1.5.3 above original H.1.5.3 and renumber the original clauses H.1.5.3 (Advantages of cross certification), H.1.5.4 (Disadvantages of cross certification), and H.1.5.5 (Risk mitigation of cross certification) as subclauses:

H.1.5.3 Advantages, Disadvantages and Risk Management of cross certification

H.1.5.3.1 Advantages of cross certification

H.1.5.3.2 Disadvantages of cross certification

H.1.5.3.3 Risk mitigation of cross certification

Clause H.1.5.1

Renumber Figure H.1 and H.2 as Figure H.6 and H.7.

Clause H.1.5.2

Renumber Figure H.3 and H.4 as Figure H.8 and H.9.

Clause H.1.6

Renumber Figure H.5 to H.10 as Figure H.10 to H.15.

Annex J

Add the following new Annex at the end of Annex J

- Entwurf -

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Annex K
(normative)

Requirements for the use of digital communication with the megawatt charging system

K.1 Overview

This Annex defines the necessary requirements, parameters and conditions for the use of digital communication with the megawatt charging system (MCS) according to IEC 61851-23-3. The associated new services MCS and MCS_BPT are derived from the DC and DC_BPT service and will use the DC schema for the messages for DC charging and DC BPT.

K.2 V2G message definition

If the MCS or MCS_BPT service is selected, the definitions and requirements in 8.3.1, 8.3.2, and 8.3.3 apply.

K.2.1 Request and response definitions

If the MCS or MCS_BPT service is selected, the message definitions and requirements in 8.3.4.2, 8.3.4.3, and 8.3.4.5 apply.

K.2.1.1 V2G session handling

If the MCS or MCS_BPT service is selected, the requirements in 8.3.4.1.1 and 8.3.4.1.2 apply.

K.2.1.1.1 V2G session pausing

If the MCS or MCS_BPT service is selected, the requirements and notes in 8.3.4.1.3 apply, except for [V2G20-2099]. Instead, the following requirement applies:

[V2G20-3088] [MCS] During a pause period with conductive charging and communication via 10BASE-T1S, the physical connection shall be maintained throughout the entire service session.

K.2.1.1.2 V2G session resumption

If the MCS or MCS_BPT service is selected, the requirements and notes in 8.3.4.1.4, 8.3.4.1.4.2, and 8.3.4.1.4.3 apply.

K.2.1.1.2.1 V2G session resumed successfully

If the MCS or MCS_BPT service is selected, the requirements and notes in 8.3.4.1.4.1 apply, except for [V2G20-2301] and [V2G20-2624]. Instead, the following requirements apply:

[V2G20-3089] [MCS] If [V2G20-1540] applies and a connection based on ISO 15118-10 has been established, the EVCC shall take care that [V2G20-1541] is fulfilled as long as no CE state A, E, EC, or EC_Aux was detected in the EVCC as defined in IEC 61851-23-3.

[V2G20-3090] [MCS] If [V2G20-2623] applies and a connection based on ISO 15118-10 has been established, the SECC shall take care that [V2G20-1058] is fulfilled as long as no CE state A, E, EC, or EC_Aux was detected in the SECC as defined in IEC 61851-23-3.

K.2.2 Complex data types

If the MCS or MCS_BPT service is selected, the definitions and requirements in 8.3.5.1, 8.3.5.2, 8.3.5.3, and 8.3.5.5 apply.

K.3 Service selection

If the MCS or MCS_BPT service is selected, the requirements in 8.4.1 and 8.4.2 apply.

K.3.1 Selection of service and service parameters

If the MCS or MCS_BPT service is selected, the requirements in 8.4.3.1 apply.

K.3.1.1 Service parameters for the MCS service

K.3.1.1.1 General

If the MCS or MCS_BPT service is selected, the requirement in 8.4.3.2.1 applies.

K.3.1.1.2 MCS service

[V2G20-3091] [MCS] The EVCC and the SECC shall implement the ServiceParameterList for MCS charging as defined in Table K.1.

Table K.1 — Configuration parameters for MCS service

ParameterName	ParameterType	Values	Description
Connector	intValue	1: MCS 2: Chaoji 3: Ultra-Chaoji 4:rMCS 5:xMCS 6:Aviation (reserved) 7:Marine (reserved)	Usage of the connector: MCS: Configuration HH according to IEC 63379. Chaoji: Configuration GG according to IEC 62196-3. Ultra Chaoji: Configuration JJ according to IEC 62196 Other values are under development/consideration.
ControlMode	IntValue	1: Scheduled 2: Dynamic	Selection of which party (SECC or EVCC) is responsible to fulfill the mobility needs of this service session.
MobilityNeedsMode	intValue	1: Mobility needs provided by EVCC 2: Mobility needs provided by SECC allowed	Indicate who can provide mobility needs information. Value 2 indicates that not only EVCC but also SECC can provide mobility-needs information (however, the EVCC shall always provide an initial mobility-needs information including DepartureTime). Value 2 can be selected only if DynamicControlMode was selected.
Pricing	intValue	0: No pricing 1: Absolute Pricing 2: Price Levels	Providing information about which pricing structure will be used in the offered schedules.

NOTE 1 Each ParameterSetID includes all parameters for a specific setup.

NOTE 2 In case a pricing method is offered that will not be used by the EVCC, the EVCC can ignore the provided information.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

- [V2G20-3092] [MCS]** In case the MCS service was selected, unless otherwise stated, anytime an element is prefixed with DC (e.g. DC_CPDReqEnergyTransferMode), it shall be used.
- [V2G20-3093] [MCS]** The SECC shall only offer MobilityNeedsMode equal to "2" when ControlMode is set to "2" (Dynamic).

K.3.1.1.2.1 MCS BPT service

- [V2G20-3094] [MCS]** The EVCC and the SECC shall implement the ServiceParameterList for MCS bidirectional power transfer as defined in Table K.2.

Table K.2 — Configuration parameters for MCS_BPT service

ParameterName	ParameterType	Values	Description
Connector	intValue	1: MCS 2: Chaoji 3: Ultra-Chaoji 4:rMCS 5:xMCS 6:Aviation (reserved) 7:Marine (reserved)	Usage of the connector: MCS: Configuration HH according to IEC 63379. Chaoji: Configuration GG according to IEC 62196-3. Ultra Chaoji: Configuration JJ according to IEC 62196 Other values are under development/consideration.
ControlMode	IntValue	1: Scheduled 2: Dynamic	Selection of which party (SECC or EVCC) is responsible to fulfill the mobility needs of this service session.
MobilityNeedsMode	intValue	1: Mobility needs provided by EVCC 2: Mobility needs provided by SECC allowed	Indicate who can provide mobility needs information. Value 2 indicates that not only EVCC but also SECC can provide mobility-needs information (however, the EVCC shall always provide an initial mobility-needs information including Departure-Time). Value 2 can be selected only if DynamicControlMode was selected.
Pricing	intValue	0: No pricing 1: Absolute Pricing 2: Price Levels	Providing information about which pricing structure will be used in the offered schedules.
BPTChannel	intValue	1: Unified 2: Separated	Type of installed power transfer channel. Unified: Single channel Separated: Dual channel
GeneratorMode	intValue	1: GridFollowing 2: GridForming	Power converter behavior. For details see the IEC/TS 62898 series.

NOTE 1 Each ParameterSetID includes all parameters for a specific setup.

NOTE 2 In case a pricing method is offered that will not be used by the EVCC, the EVCC can ignore the provided information.

- [V2G20-3095] [MCS]** In case the MCS BPT service was selected, unless otherwise stated, anytime an element is prefixed with BPT or DC (e.g. BPT_DC_CPDReqEnergyTransferMode), it shall be used. In case both elements are available exclusively, BPT takes precedence.

The following requirements apply in case of MCS_BPT channel is equal to "separated" (e.g. Dual channel) and the energy transfer needs to move from a charging phase to a discharging phase (or vice-versa).

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****[V2G20-3096] [MCS]**

In case a service was selected where parameter BPTChannel was set to "2" (Separated), the SECC shall apply a power of 0 kW until contactors position are ready for the new phase.

In DC energy transfer mode, one could argue that the BPT Channel parameter might not be necessary, as the switch control operation is performed by the SECC. However, in case of a negotiated power profile (scheduled control mode), the EVCC should take into account the physical architecture (e.g. by planning 0 kW steps between charging and discharging phases).

[V2G20-3097] [MCS]

In case of bidirectional power transfer where parameter BPTChannel was set to "2" (Separated), both SECC and EVCC shall include 0 kW steps when switching from charging to discharging or vice versa.

[V2G20-3098] [MCS]

The SECC shall only offer MobilityNeedsMode equal to "2" when ControlMode is set to "2" (Dynamic).

K.4 V2G communication timing

If the MCS or MCS_BPT service is selected, clauses 8.5.1 and 8.5.2 apply. The timing concepts specified in 8.5.3 for the DC and DC_BPT service apply for the MCS and MCS_BPT service as well.

K.4.1 Message sequence and communication session

If the MCS or MCS_BPT service is selected, the requirements in 8.5.4.1 apply. The requirements specified in 8.5.4.3 for the DC and DC_BPT service apply for the MCS and MCS_BPT service as well.

K.4.2 Session setup and ready to charge

If the MCS or MCS_BPT service is selected, the timing parameters and requirements in 8.5.5.1 apply. The timing parameters and requirements specified in 8.5.5.2 for the DC and DC_BPT service apply for the MCS and MCS_BPT service as well.

K.4.3 V2G message synchronization for MCS with IEC 61851-23-3 signalling

K.4.3.1 Overview

MCS based energy transfer control used the charge enable function according to IEC 61851-23-3. For this, the messaging on application layer is synchronized with the CE states defined in IEC 61851-23-3:202X, Annex CC.

In this subclause, terms and definitions in requirements are applied as defined in ISO 15118-10 and IEC 61851-23-3:202X, Annex CC.

Figure K.1 shows an example for DC energy transfer with HLC-C in relation to service session and phases of data link setup, V2G setup and V2G power transfer loop during a V2G communication session.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

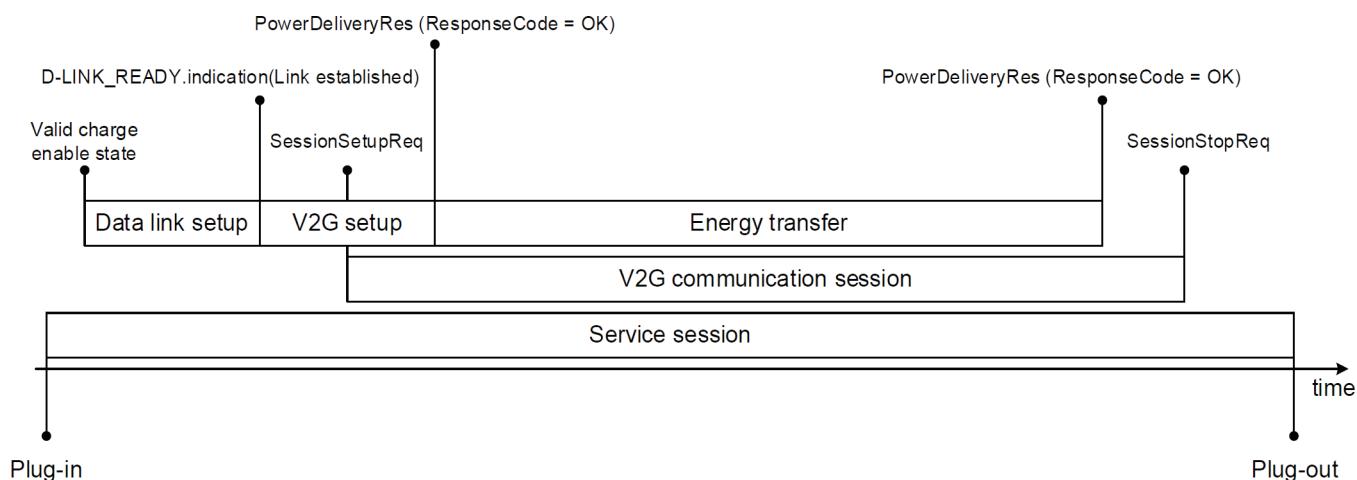


Figure K.1 — Energy transfer in relation to service session

The V2G power transfer loop is defined as V2G messaging phase for controlling the energy transfer process by the ISO 15118 series in normal operation. The power transfer phase under control of the ISO 15118 series is defined as high level communication charging (HLC-C).

The entry and exit conditions for the V2G power transfer loop are as follows:

- entry condition: PowerDeliveryRes message with parameter ResponseCode equal to OK after PowerDeliveryReq with ChargeProgress equals "Start";
- exit condition: PowerDeliveryRes with parameter ResponseCode equal to OK after PowerDeliveryReq with ChargeProgress equals "Stop".

Besides the requirements for request-response message pairs and request-response message sequences as defined in 8.6.4, the EVCC and the SECC shall conform to the requirements as defined in 8.5.8.2, 8.5.8.3, and 8.5.8.4.

K.4.3.2 Common requirements for AC, DC and MCS

The requirements in 8.5.6.2 shall be applied, except for [V2G20-843] and [V2G20-1404].

Instead, the following requirements apply:

[V2G20-3099] [MCS] An ISO 15118-enabled EV shall conform to IEC 61851-23-3.

[V2G20-3100] [MCS] An ISO 15118-enabled EVSE shall conform to IEC 61851-23-3.

K.4.3.3 MCS specific requirements

The following requirements apply for the EVCC.

[V2G20-3101] [MCS] After receiving a ScheduleExchangeRes with EVSEProcessing set to "Finished" and before sending a DC_CableCheckReq message, the EVCC shall change to CE State C or C_Aux as defined in IEC 61851-23-3.

[V2G20-3102] [MCS] After sending a PowerDeliveryReq message with ChargeProgress equal to "Stop" and receiving the corresponding PowerDeliveryRes message, the EVCC shall change to CE State B or B_Aux as defined in IEC 61851-23-3 before sending the next request message.

[V2G20-3103] [MCS] If **[V2G20-3101] [MCS]** applies and no error has been identified, the EVCC shall not change the CE State until **[V2G20-3102] [MCS]** applies.

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

The following requirements of 8.5.6.4 apply for the EVCC during a standby period.

[V2G20-1380], [V2G20-2119], [V2G20-1381], and [V2G20-1383].

The following requirements apply for the SECC.

[V2G20-3104] [MCS] The SECC shall keep S_S3 closed from the start of data link setup until end of V2G communication session.

The SECC waits for positive authorization and availability of energy before entering the charging loop.

[V2G20-3105] [MCS] After receiving a DC_CableCheckReq message, the SECC shall monitor the CE State and start the V2G_SECC_Msg_Performance_Timer.

[V2G20-3106] [MCS] The SECC shall respond with DC_CableCheckRes containing "ResponseCode = OK" within V2G_SECC_Msg_Performance_Time according to Table 215, if the SECC measures a CE State C or C_Aux.

[V2G20-3107] [MCS] The SECC shall respond with DC_CableCheckRes containing "ResponseCode = "FAILED" within V2G_SECC_Msg_Performance_Time according to Table 215, if the SECC measures no CE State C or C_Aux.

[V2G20-3108] [MCS] After sending a PowerDeliveryRes message with parameter ResponseCode set to "OK" in response to a PowerDeliveryReq with parameter ChargeProgress set to "Stop", the SECC shall try to measure CE state B or B_Aux.

[V2G20-3109] [MCS] After receiving a DC_WeldingDetectionReq message or a SessionStopReq message, the SECC shall wait for a maximum of V2G_SECC_Msg_Performance_Time to measure CE state B or B_Aux.

[V2G20-3110] [MCS] After receiving a DC_WeldingDetectionReq message or a SessionStopReq message, the SECC shall send the corresponding response message with parameter ResponseCode set to "OK" within V2G_SECC_Msg_Performance_Time according to Table 103, if CE State B or B_Aux was measured.

[V2G20-3111] [MCS] After receiving a DC_WeldingDetectionReq message or a SessionStopReq message, the SECC shall send the corresponding response message with parameter ResponseCode set to "FAILED" within V2G_SECC_Msg_Performance_Time according to Table 103, if CE State B or B_Aux was not measured.

K.4.3.4 MCS reverse power transfer specific requirements

K.4.3.4.1 General

In the discharging services, EVCC and SECC shall align to IEC 61851-23-3 signalling in the same way as in the charging services. Until the discharging service is added in IEC 61851-23-3, it is defined as an extension within this document. Basic status definitions between charging and discharging are similar, but trigger conditions for charging and discharging loops are defined for reverse power transfer system. It shall be given by HLC control under the condition of IEC 61851-23-3 signalling agreement.

K.4.3.4.2 BPT specific requirements for MCS

The common requirements defined in 8.5.8.2 shall be applied except for **[V2G20-3099] [MCS]** and **[V2G20-3100] [MCS]**. Instead, the following requirements apply.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

[V2G20-3112] [MCS] ISO 15118 enabled EVCC shall conform to IEC 61851-23-3 in case of charging. Also, ISO 15118 enabled EVCC shall similarly work as defined in IEC 61851-23-3 in case of discharging.

[V2G20-3113] [MCS] ISO 15118 enabled SECC shall conform to IEC 61851-23-3 in case of charging. Also, ISO 15118 enabled SECC shall similarly work as the EVSE defined in IEC 61851-23-3 in case of discharging.

K.5 Message sequencing and error handling

If the MCS or MCS_BPT service is selected, clauses 8.6.1 and 8.6.2 apply. Furthermore, the DC message sequence diagram specified in 8.6.6 applies for the MCS as well.

K.5.1 ResponseCode handling

If the MCS or MCS_BPT service is selected, the requirements in 8.6.3.1 apply. The requirements specified in 8.6.3.3 for the DC and DC_BPT service apply for the MCS and MCS_BPT service as well.

K.5.2 Request-response message sequence requirements

If the MCS or MCS_BPT service is selected, the requirements in 8.6.4.1 apply.

K.5.2.1 MCS requirements

The requirements in 8.6.4.3 shall be applied, except for [V2G20-1650].

Instead, the following requirement applies:

[V2G20-3114] [MCS] MCS shall use 10BASE-T1S communication exclusively.

K.5.2.2 EVCC

If the MCS or MCS_BPT service is selected, the requirements in 8.6.4.5.1 and 8.6.4.5.2 apply.

K.5.2.2.1 Message flow

If the MCS or MCS_BPT service is selected, the requirements in 8.6.4.5.3.1 apply.

K.5.2.2.1.1 MCS Message flow

For MCS and MCS_BPT, the following requirements apply for the EVCC.

[V2G20-3115] [MCS] After receiving the SessionSetupRes with ResponseCode equal to "OK", the EVCC shall send the proper DC_ChargeParameterDiscoveryReq while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time, in case the EVCC resumes a previously paused V2G communication session.

NOTE 1 In case of a resumed session, the authorization is not required, as authorization details of the previous communication session are valid for the whole service session, see [V2G20-1844].

[V2G20-3116] [MCS] If EVCC is using ServiceName= MCS or MCS_BPT in Table 204, after receiving the ScheduleExchangeRes with "ResponseCode = OK", and EVSEProcessing set to "Finished", the EVCC shall send a DC_CableCheckReq within V2G_EVCC_Sequence_Performance_Time according to Table 217.

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****[V2G20-3117] [MCS]**

After receiving the DC_CableCheckRes with "ResponseCode = OK" and EVSEProcessing set to "Ongoing", the EVCC shall send another DC_CableCheckReq within V2G_EVCC_Sequence_Performance_Time according to Table 217.

[V2G20-3118] [MCS]

After receiving the DC_CableCheckRes with "ResponseCode = OK", and EVSEProcessing set to "Finished", the EVCC shall send a DC_PreChargeReq within V2G_EVCC_Sequence_Performance_Time according to Table 217.

[V2G20-3119] [MCS]

After receiving the DC_PreChargeRes with "ResponseCode = OK", the EVCC shall send a DC_PreChargeReq with EVProcessing set to "Ongoing" within V2G_EVCC_Sequence_Performance_Time according to Table 217 while the precharge process is not finished.

[V2G20-3120] [MCS]

After receiving the DC_PreChargeRes with "ResponseCode = OK", the EVCC shall send a DC_PreChargeReq with EVProcessing set to "Finished" within V2G_EVCC_Sequence_Performance_Time according to Table 217 when the precharge process is finished.

[V2G20-3121] [MCS]

After having received a DC_PreChargeRes with "ResponseCode = OK" as a response to a DC_PreChargeReq with EVProcessing set to 'Finished', the EVCC shall send a PowerDeliveryReq within V2G_EVCC_Sequence_Performance_Time according to Table 215.

[V2G20-3122] [MCS]

If EVCC uses ServiceName = MCS or MCS_BPT from Table 204, after receiving the PowerDeliveryRes with "ResponseCode = OK" or "ResponseCode = WARNING_PowerToleranceNotConfirmed", the EVCC shall send a DC_ChargeLoopReq within V2G_EVCC_Sequence_Performance_Time according to Table 217 to start the energy transfer, a schedule renegotiation or enter a standby period.

During standby both EV and EVSE contactors are to stay closed. The standby concept is solely used as communication state within this document and therefore is not reflected in related documents, e.g. IEC 61851-23-3.

[V2G20-3123] [MCS]

If the EVCC wants to continue the energy transfer and received the DC_ChargeLoopRes with "ResponseCode = OK", the EVCC shall send another DC_ChargeLoopReq within V2G_EVCC_Sequence_Performance_Time according to Table 217.

[V2G20-3124] [MCS]

If the EVCC wants to stop the energy transfer and received the DC_ChargeLoopRes with "ResponseCode = OK", the EVCC shall send a PowerDeliveryReq with ChargeProgress = "Stop" within V2G_EVCC_Sequence_Performance_Time according to Table 215.

[V2G20-3125] [MCS]

If the EVCC wants to enter a standby phase and received the DC_ChargeLoopRes with "ResponseCode = OK", the EVCC shall send a PowerDeliveryReq with ChargeProgress = "Standby" within V2G_EVCC_Sequence_Performance_Time according to Table 215.

[V2G20-3126] [MCS]

If the EVCC is using ServiceName = MCS or MCS_BPT in Table 204, after receiving the PowerDeliveryRes with "ResponseCode = OK" and if the previous PowerDeliveryReq message has ChargeProgress = "Stop", the EVCC shall send a DC_WeldingDetectionReq within V2G_EVCC_Sequence_Performance_Time according to Table 217.

[V2G20-3127] [MCS]

After receiving the DC_WeldingDetectionRes with "ResponseCode = OK", the EVCC shall send a DC_WeldingDetectionReq with EVProcessing set to "Ongoing" within V2G_EVCC_Sequence_Performance_Time according to Table 217 while the welding detection process is not finished.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

[V2G20-3128] [MCS]

After receiving the DC_WeldingDetectionRes with "ResponseCode = OK", the EVCC shall send a DC_WeldingDetectionReq with EVProcessing set to "Finished" within V2G_EVCC_Sequence_Performance_Time according to Table 217 when the welding detection process is finished.

[V2G20-3129] [MCS]

After receiving the DC_WeldingDetectionRes message with "ResponseCode = OK", the EVCC shall send a SessionStopReq within V2G_EVCC_Sequence_Performance_Time according to Table 215.

K.5.2.3 SECC

If the MCS or MCS_BPT service is selected, the requirements in 8.6.4.6.1 and 8.6.4.6.2 apply.

K.5.2.3.1 Message flow

If the MCS or MCS_BPT service is selected, the requirements in 8.6.4.6.3.1 apply.

K.5.2.3.1.1 MCS Message flow

For MCS and MCS_BPT, the following requirements apply for the SECC.

[V2G20-3130] [MCS]

After receiving the ScheduleExchangeReq, the SECC shall respond with a ScheduleExchangeRes with EVSEProcessing set to "Finished" within V2G_SECC_Msg_Performance_Time according to Table 215, if the process is finished. The next allowed request shall be DC_CableCheckReq if ServiceName= MCS or MCS_BPT in Table 204 was selected. The V2G_SECC_Sequence_Timeout is set according to Table 217.

[V2G20-3131] [MCS]

After receiving the DC_CableCheckReq, the SECC shall respond with a DC_CableCheckRes with EVSEProcessing set to "Ongoing" within V2G_SECC_Msg_Performance_Time according to Table 217, while the cable check process is still ongoing. The next allowed request shall be DC_CableCheckReq and the V2G_SECC_Sequence_Timeout is set according to Table 217.

[V2G20-3132] [MCS]

After receiving the DC_CableCheckReq, the SECC shall respond with a DC_CableCheckRes with EVSEProcessing set to "Finished" within V2G_SECC_Msg_Performance_Time according to Table 217, if the cable check process is finished. The next allowed request shall be DC_PreChargeReq and the V2G_SECC_Sequence_Timeout is set according to Table 217.

[V2G20-3133] [MCS]

After receiving the DC_PreChargeReq with EVProcessing set to "Ongoing", the SECC shall respond with a DC_PreChargeRes within V2G_SECC_Msg_Performance_Time according to Table 217. The next allowed request shall be DC_PreChargeReq and the V2G_SECC_Sequence_Timeout is set according to Table 217.

[V2G20-3134] [MCS]

After receiving the DC_PreChargeReq with EVProcessing set to "Finished", the SECC shall respond with a DC_PreChargeRes within V2G_SECC_Msg_Performance_Time according to Table 217. The next allowed request shall be PowerDeliveryReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-3135] [MCS]

If the PowerDeliveryReq received has ChargeProgress = "Start" and ServiceName = MCS or MCS_BPT in Table 204 was selected, the next allowed request shall be DC_ChargeLoopReq and the V2G_SECC_Sequence_Timeout is set according to Table 217.

[V2G20-3136] [MCS]

After receiving the DC_ChargeLoopReq, the SECC shall respond with a DC_ChargeLoopRes with "ResponseCode = OK" within V2G_SECC_Msg_Performance_Time according to Table 217. The next allowed request shall be DC_ChargeLoopReq or PowerDeliveryReq and the V2G_SECC_Sequence_Timeout is set according to Table 217.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

[V2G20-3137] [MCS]

If ServiceName = MCS or MCS_BPT in Table 204 is used, and the PowerDeliveryReq received has ChargeProgress = "Stop", the next allowed request shall be DC_WeldingDetectionReq and the V2G_SECC_Sequence_Timeout is set according to Table 217.

[V2G20-3138] [MCS]

After receiving the DC_WeldingDetectionReq with EVProcessing set to "Ongoing", the SECC shall respond with a DC_WeldingDetectionRes within V2G_SECC_Msg_Performance_Time according to Table 217. The next allowed request shall be DC_WeldingDetectionReq and the V2G_SECC_Sequence_Timeout is set according to Table 217.

[V2G20-3139] [MCS]

After receiving the DC_WeldingDetectionReq with EVProcessing set to "Finished", the SECC shall respond with a DC_WeldingDetectionRes within V2G_SECC_Msg_Performance_Time according to Table 217. The next allowed request shall be SessionStopReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-3140] [MCS]

The SECC shall be able to set the parameter EVSENNotification in EVSEStatus to "ServiceRenegotiation" only in DC_ChargeLoopRes.

[V2G20-3141] [MCS]

If the first ServiceDiscoveryRes of the service session had the parameter ServiceRenegotiationSupported set to "True" and the SECC decides to perform a ServiceRenegotiation for adapting its service offering, it shall set the parameter EVSENNotification in EVSEStatus to "ServiceRenegotiation" in DC_ChargeLoopRes.

K.5.3 Multiplexed communication

If the MCS or MCS_BPT service is selected, the requirements in 8.6.5, including its subclauses, shall be applied, except for [V2G20-1040]. Instead, the following requirement applies:

[V2G20-3142] [MCS]

If ServiceName = MCS or MCS_BPT in Table 204 is used , the conditions defined for the CE state within the message sequence requirements shall only apply to the main stream EXI encoded messages with V2GTP payload types in the range 0x8001 up to 0x80FF.

Annex J

Add the following new Annex at the end of Annex J (after the new Annex K)

- Entwurf -

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Annex L
(normative)

Requirements for the use of an AC DER service

L.1 Overview

It is undeniable that this decade will be marked by an increasing number of V2G use cases and projects: from feeding back energy to a home environment to using a fleet of EVs as a virtual power plant to peak-shaving power demand or even relying on a swarm of EVs to sustain grid events, the possibilities are vast. In contrast to the well-known charging scenario with an EV, feeding back to the grid comes with an increased number of requirements and complexity.

Fortunately, feeding back energy to the grid is not a new and unknown use case, as, for decades, there have been grid assets that provide this service, such as hydro power generators, wind generators, photovoltaic panels, and battery storage devices. These are called distributed energy resources (DER).

This means that there are already standards that provide normative requirements for how DER must behave when feeding energy to the grid, e.g.:

- IEEE 1547-2018
- EN 50549
- UK G98 and G99
- VDE-AR-N 4105
- AS/NZS 4777

This Annex considers all the mentioned grid code standards and the SAE J3072 requirements, extending the functionality of ISO 15118-20 to include attributes and functions to allow for a standardized vehicle-to-grid interconnection.

As the technical requirements for the system design have not yet been finalized in the relevant technical committees e.g. in ISO and IEC/SAE/UL/..., different technical concepts are conceivable. The aim of this Annex is to serve all system designs defined by the relevant technical committees, e.g. IEC TC 69 (IEC 61851-1, under maintenance), ISO TC 22 SC 37 (ISO 5474-2, under maintenance).

Once the functions on the EV and EVSE side have been finalized by the relevant technical committees, it may be possible to optimize the parameter lists.

L.2 V2G message definition

If the AC DER service is selected, the definitions and requirements in 8.3.1, 8.3.2, and 8.3.3 apply.

L.2.1 Request and response definitions

If the AC DER service is selected, the message definitions and requirements in 8.3.4.1, 8.3.4.2, and 8.3.4.3 apply.

L.2.1.1 AC DER messages

L.2.1.1.1 General

The following messages are based on the AC message set but define the AC DER message set. If not stated otherwise, the requirements of the AC message set specified in 8.3.4.4 apply for the AC DER service as well.

L.2.1.1.2 AC_ChargeParameterDiscoveryReq/Res for the AC DER service

After being authorized for charging at the EVSE (SECC) the EVCC and the SECC negotiate the energy transfer parameters with the AC_ChargeParameterDiscovery message pair.

Concepts treated for an optimal supply of energy that corresponds to the customer needs:

When using scheduled control mode, the energy transfer parameters negotiation that precedes the delivery of energy or may be engaged during the energy delivery phase is destined to ensure that the user will be satisfied while at the same time ensuring that the energy will effectively be available and fall within the capacity of power supply grid at the local level (private network) and at the regional level (public network). This required negotiation will become more and more necessary as the number of EVs increase, as well as an increase in volatility of local renewable energy production.

When using the dynamic control mode, the energy transfer parameters can be changed dynamically while in the charging loop, depending on the need of the EVSE.

L.2.1.1.2.1 AC_ChargeParameterDiscoveryReq for the AC DER service

By sending the AC_ChargeParameterDiscoveryReq message the EVCC provides its energy transfer parameters to the SECC. This message provides status information about the EV, i.e. the capabilities of the EV charging system.

[V2G20-3143] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.1 and Figure L.1.

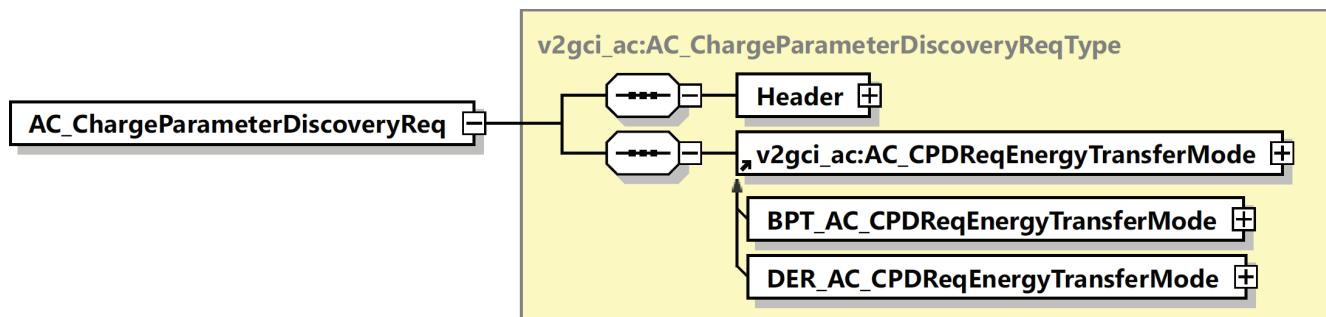


Figure L.1 — Schema diagram – AC_ChargeParameterDiscoveryReq for the AC DER service

The elements of this message are used according to Table L.1.

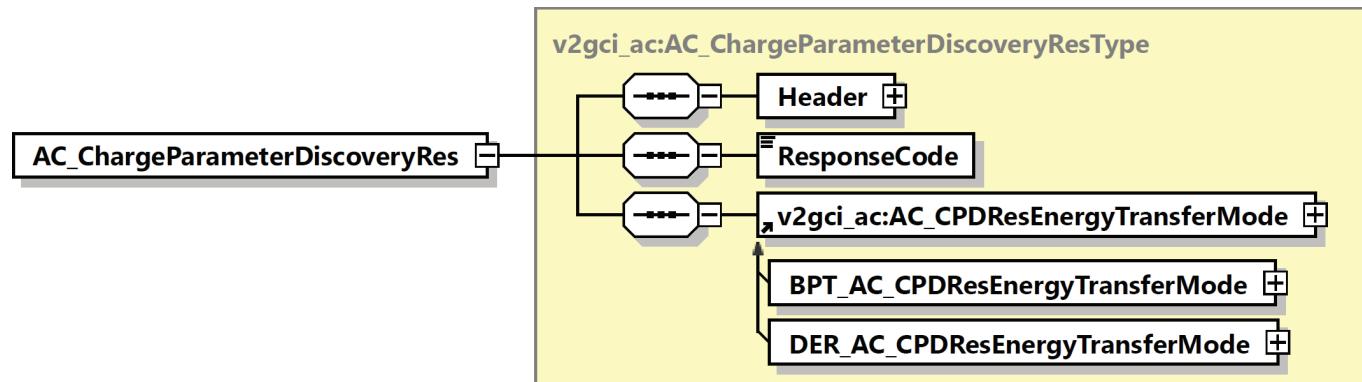
Table L.1 — Semantics and type definition for AC_ChargeParameterDiscoveryReq for the AC DER service

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
AC_CPDReqEnergyTransferMode	complexType: AC_CPDReqEnergyTransferModeType refer to 8.3.5.4.1	This element is used by the EVCC for initiating the target setting process for AC energy transfer.
BPT_AC_CPDReqEnergyTransferMode	complexType: BPT_AC_CPDReqEnergyTransferModeType refer to 8.3.5.4.7.1	This element is used by the EVCC for initiating the target setting process for AC BPT.
DER_AC_CPDReqEnergyTransferMode	complexType: DER_AC_CPDReqEnergyTransferModeType refer to L.2.2.1.2	This element is used by the EVCC for initiating the target setting process for AC DER.

L.2.1.1.2.2 AC_ChargeParameterDiscoveryRes for the AC DER service

With the AC_ChargeParameterDiscoveryRes message the SECC provides applicable charge parameters from the grid's perspective.

[V2G20-3144] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.2 and Figure L.2.

**Figure L.2 — Schema diagram – AC_ChargeParameterDiscoveryRes for the AC DER service**

The elements of this message are used according to Table L.2.

Table L.2 — Semantics and type definition for AC_ChargeParameterDiscoveryRes for the AC DER service

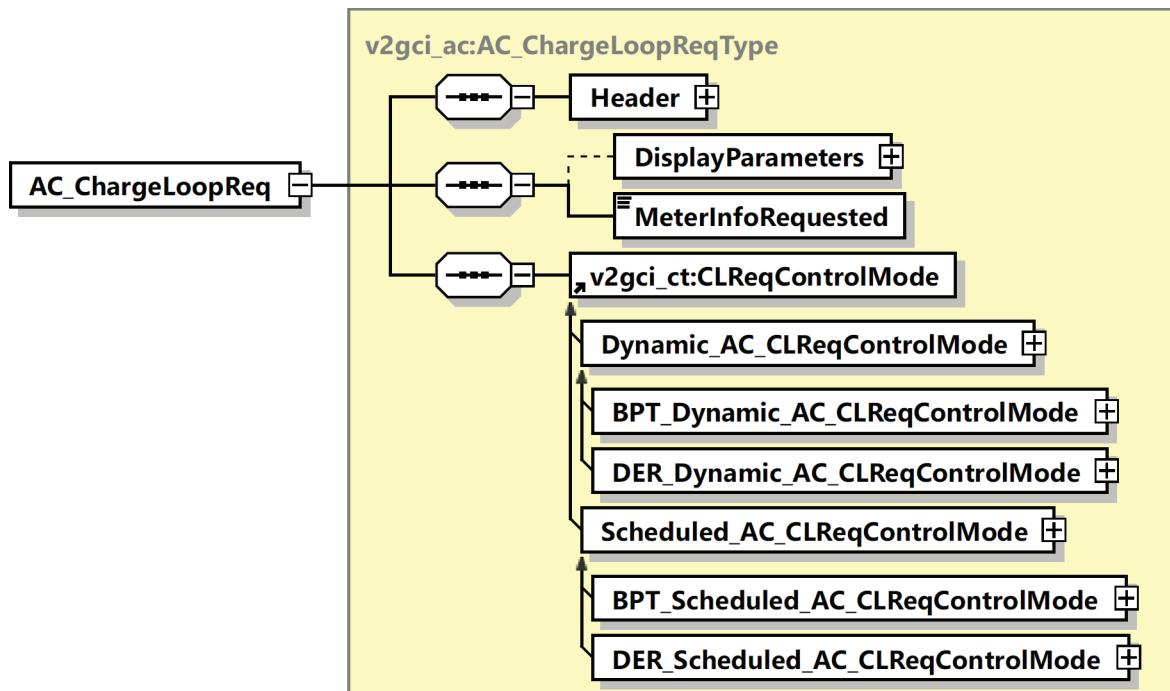
Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgement status of any of the V2G messages received by the SECC.
AC_CPDResEnergyTransferMode	complexType: AC_CPDResEnergyTransferModeType refer to 8.3.5.4.2	This element is used by the SECC for initiating the target setting process for AC energy transfer.
BPT_AC_CPDResEnergyTransferMode	complexType: BPT_AC_CPDResEnergyTransferModeType refer to 8.3.5.4.7.2	This element is used by the SECC for initiating the target setting process for AC BPT.
DER_AC_CPDResEnergyTransferMode	complexType: DER_AC_CPDResEnergyTransferModeType refer to L.2.2.1.3	This element is used by the SECC for initiating the target setting process for AC DER.

L.2.1.1.3 AC_ChargeLoopReq/Res for the AC DER service

The AC_ChargeLoop message pair provides continuous data exchange between SECC and EVCC. Additionally, it allows sanity checks on the meter readings provided by the SECC.

L.2.1.1.3.1 AC_ChargeLoopReq for the AC DER service

[V2G20-3145] [DER] The EVCC and the SECC shall implement the message elements as defined in as defined in Table L.3 and Figure L.3.

**Figure L.3 — Schema diagram – AC_ChargeLoopReq for the AC DER service**

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

The elements of this message are used according to Table L.3.

Table L.3 — Semantics and type definition for AC_ChargeLoopReq for the AC DER service

Element	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
DisplayParameters	complexType: DisplayParametersType refer to 8.3.5.3.28	Optional Parameters that may be displayed on the EVSE or any other user interface which is connected directly or indirectly to the EVSE. They shall under no circumstances influence the V2G communication session.
MeterInfoRequested	simpleType: xs:boolean	When this parameter is set to true, the next AC_ChargeLoopRes shall include the MeterInfo.
Dynamic_AC_CLReqControlMode	complexType: Dynamic_AC _CLReqControlModeType refer to 8.3.5.4.3	This element is used by the EVCC for offering and setting parameters for dynamic control mode energy transfer.
BPT_Dynamic_AC_CLReqControlMode	complexType: BPT_Dynamic_AC _CLReqControlModeType refer to 8.3.5.4.7.3	This element is used by the EVCC for offering and setting parameters for dynamic control mode BPT.
DER_Dynamic_AC_CLReqControlMode	complexType: DER_Dynamic_AC _CLReqControlModeType refer to L.2.2.1.4	This element is used by the EVCC for offering and setting parameters for dynamic control mode DER energy transfer.
Scheduled_AC_CLReqControlMode	complexType: Scheduled_AC _CLReqControlModeType refer to 8.3.5.4.4	This element is used by the EVCC for offering and setting parameters for scheduled control mode energy transfer.
BPT_Scheduled_AC_CLReqControlMode	complexType: BPT_Scheduled_AC _CLReqControlModeType refer to 8.3.5.4.7.4	This element is used by the EVCC for offering and setting parameters for scheduled control mode BPT.
DER_Scheduled_AC_CLReqControlMode	complexType: DER_Scheduled_AC _CLReqControlModeType refer to L.2.2.1.5	This element is used by the EVCC for offering and setting parameters for scheduled control mode DER energy transfer.

L.2.1.1.3.2 AC_ChargeLoopRes for the AC DER service

[V2G20-3146] [DER] The EVCC and the SECC shall implement the message elements as defined in as defined in Table L.4 and Figure L.4.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

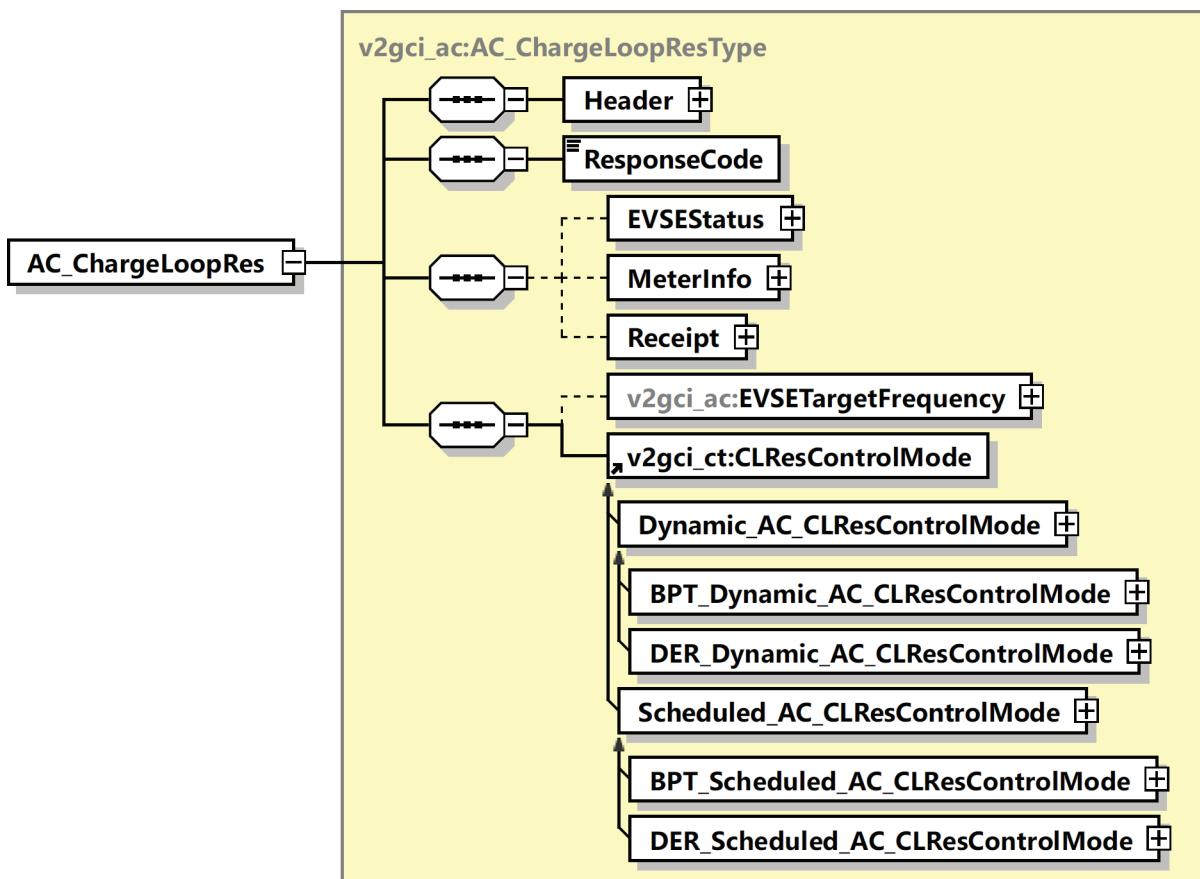


Figure L.4 — Schema diagram - AC_ChargeLoopRes for the AC DER service

The elements of this message are used according to Table L.4.

Table L.4 — Semantics and type definition for AC_ChargeLoopRes for the AC DER service

Element	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgement status of any of the V2G messages received by the SECC.
EVSEStatus	complexType: EVSEStatusType refer to 8.3.5.3.26	Optional: This element is used by the SECC for indicating the EVSE status and for signaling an event the SECC expects the EVCC to react to.
MeterInfo	complexType: MeterInfoType refer to 8.3.5.3.6	Optional: Includes the energy charged during this service session and other meter relevant data.
Receipt	complexType: ReceiptType Refer to 8.3.5.3.59	Optional: Receipt related information.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table L.4 (continued)

Element	Type	Semantics
EVSETargetFrequency	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target frequency requested by the EVSE
Dynamic_AC_CLResControlMode	complexType: Dynamic_AC_CLResControlModeType refer to 8.3.5.4.5	This element is used by the SECC for offering and setting parameters for dynamic control mode energy transfer.
BPT_Dynamic_AC_CLResControlMode	complexType: BPT_Dynamic_AC_CLResControlModeType refer to 8.3.5.4.7.5	This element is used by the SECC for offering and setting parameters for dynamic control mode charging and discharging.
DER_Dynamic_AC_CLResControlMode	complexType: DER_Dynamic_AC_CLResControlModeType refer to L.2.2.1.6	This element is used by the SECC for offering and setting parameters for dynamic control mode DER energy transfer.
Scheduled_AC_CLResControlMode	complexType: Scheduled_AC_CLResControlModeType refer to 8.3.5.4.6	This element is used by the SECC for offering and setting parameters for scheduled control mode energy transfer.
BPT_Scheduled_AC_CLResControlMode	complexType: BPT_Scheduled_AC_CLResControlModeType refer to 8.3.5.4.7.5	This element is used by the SECC for offering and setting parameters for scheduled control mode charging and discharging.
DER_Scheduled_AC_CLResControlMode	complexType: DER_Scheduled_AC_CLResControlModeType refer to L.2.2.1.7	This element is used by the SECC for offering and setting parameters for scheduled control mode DER energy transfer.

[V2G20-3147] [DER] If the AC DER service has been selected, the SECC shall send EVSETargetFrequency values only in situations when the GridNominalFrequency is no longer the desired equilibrium point.

L.2.2 Complex data types

The definitions and requirements in 8.3.5.1, 8.3.5.2, and 8.3.5.3 apply to the AC DER message set.

L.2.2.1 AC DER complex data types

L.2.2.1.1 General

The AC DER message set is based on the AC message set. If not stated otherwise, the requirements of the complex data types of the AC message set specified in 8.3.5.4 apply for the AC DER service as well.

L.2.2.1.2 DER_AC_CPDReqEnergyTransferModeType

[V2G20-3148] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.5 and Figure L.5.

- Entwurf -

E DIN EN ISO 15118-20/A1:2025-02
 ISO 15118-20:2022/DAM 1:2024(en)

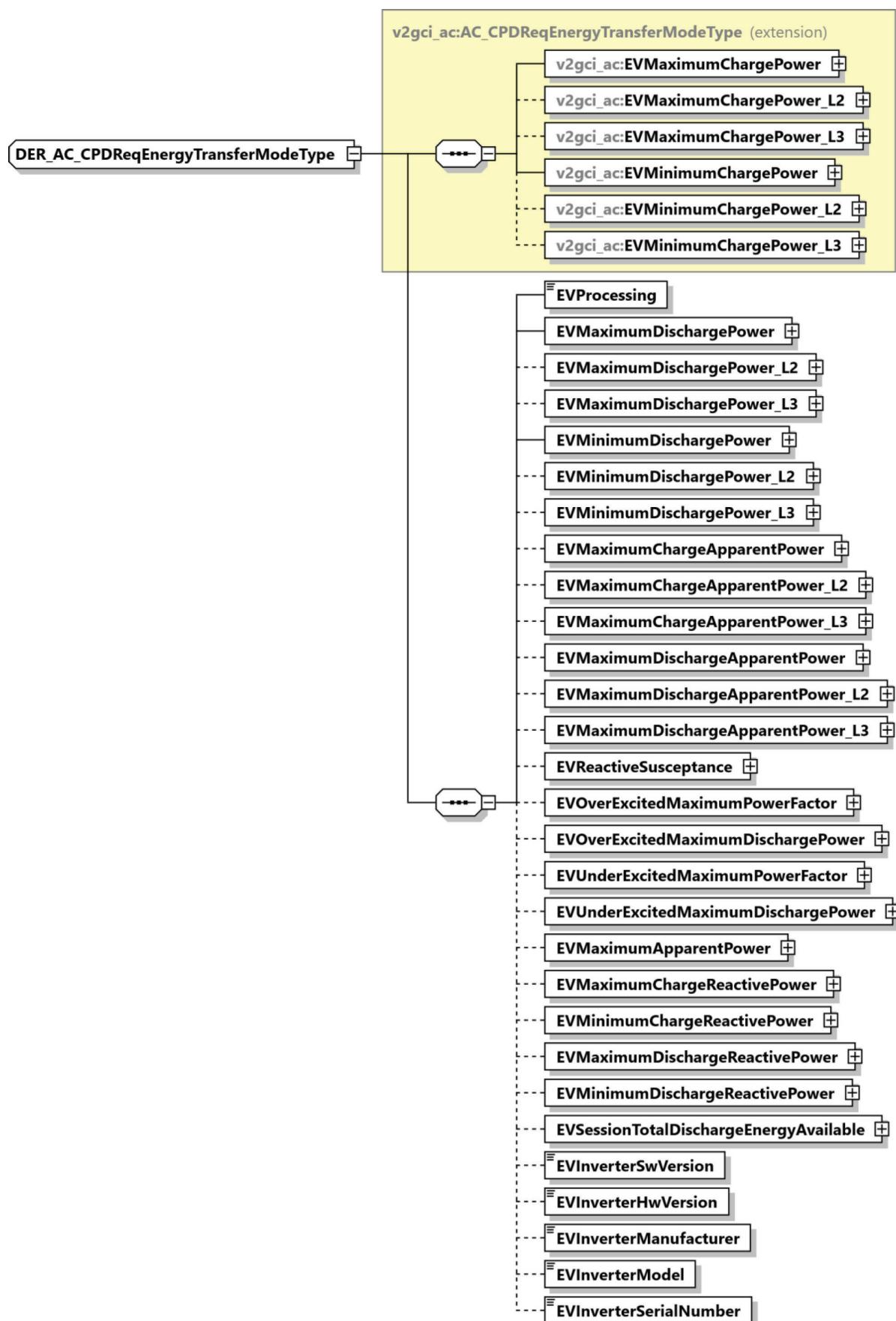


Figure L.5 — Schema diagram – DER_AC_CPDReqEnergyTransferModeType

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

The elements of this message are used according to Table L.5.

Table L.5 — Semantics and type definition for DER_AC_CPDReqEnergyTransferModeType

Element Name	Type	Semantics
EVMaximumChargePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Rated maximum absorbed active power supported by the EV at unity power factor. Corresponds to the EV.DSTO.ChaVAMaxRtg attribute in IEC 61850-7-420:2021.
EVMinimumChargePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Rated minimum absorbed active power supported by the EV at unity power factor. Corresponds to the EV.DSTO.DschWMinRtg attribute in IEC 61850-7-420:2021.
EVProcessing	simpleType: processingType enumeration refer to Annex A for the type definition	Parameter indicating whether the EVCC has finished processing the information provided by the SECC in the previous response message.
EVMaximumDischargePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Rated maximum injected active power supported by the EV at unity power factor. Corresponds to the EV.DSTO.DschVAMaxRtg attribute in IEC 61850-7-420:2021.
EVMinimumDischargePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Rated minimum injected active power supported by the EV at unity power factor. Corresponds to the EV.DSTO.DschWMinRtg attribute in IEC 61850-7-420:2021.
EVMaximumChargeApparentPower*	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Rated maximum absorbed apparent power supported by the EV in va. Corresponds to the EV.DSTO.ChaVAMaxRtg attribute in IEC 61850-7-420:2021.
EVMaximumDischargeApparentPower*	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Rated maximum injected apparent power supported by the EV in va. Corresponds to the EV.DSTO.DschVAMaxRtg attribute in IEC 61850-7-420:2021.
EVReactiveSusceptance	complexType: RationalNumberType refer to 8.3.5.3.8	Optional It measures the susceptibility of a circuit to reactance, and it is measured in Siemens (S). Corresponds to the EV.DEGEN.SuscRtg attribute in IEC 61850-7-420:2021.
EVOverExcitedMaximumPowerFactor	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV maximum power factor configured to satisfy injecting (over excited) the required minimum reactive power. Corresponds to the EV.DSTO.OvPFRtg attribute in IEC 61850-7-420:2021.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table L.5 (continued)

Element Name	Type	Semantics
EVOverExcitedMaximumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Maximum injected active power supported by the EV at the configured over-excited power factor (EVOverExcitedPowerFactor). It can also be defined as the Rated EV maximum discharge power at the rated minimum injectable reactive power value. This means that if the EV is providing reactive power support, and it is requested to discharge at max power (e.g. to satisfy an EMS request), the EV may override the request and discharge up to EVOverExcitedMaximumDischargePower: going over this value would result in the inability to continue injecting the needed minimum reactive power. Corresponds to the EV.DSTO.WOvPFRtg attribute in IEC 61850-7-420:2021.
EVUnderExcitedMaximumPowerFactor	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV maximum power factor configured to satisfy injecting (over excited) the required minimum reactive power. Corresponds to the EV.DSTO.UnPFRtg attribute in IEC 61850-7-420:2021.
EVUnderExcitedMaximumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Maximum injected active power supported by the EV at configured under-excited power factor (EVUnderExcitedPowerFactor). It can also be defined as the rated EV maximum discharge power at the rated minimum absorbable reactive power value. This means that if the EV is providing reactive power support, and it is requested to discharge at max power (e.g. to satisfy an EMS request), the EV may override the request and discharge up to EVUnderExcitedMaximumDischargePower: going over this value would result in the inability to continue absorbing the needed minimum reactive power. Corresponds to the EV.DSTO.WUnPFRtg attribute in IEC 61850-7-420:2021.
EVMaximumApparentPower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Rated maximum total apparent power supported by the EV in va. Corresponds to the EV.DSTO.VAMaxRtg attribute in IEC 61850-7-420:2021.
EVMaximumChargeReactivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Rated maximum absorbed reactive power supported by the EV in vars Corresponds to the EV.DSTO.ChaAvarRtg attribute in IEC 61850-7-420:2021.
EVMinimumChargeReactivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Rated minimum absorbed reactive power supported by the EV in vars. Corresponds to the EV.DSTO.ChaAvarMinRtg attribute in IEC 61850-7-420:2021.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table L.5 (continued)

Element Name	Type	Semantics
EVMaximumDischargeReactivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Rated maximum injected reactive power supported by the EV in vars. Corresponds to the EV.DSTO.DschIvarRtg attribute in IEC 61850-7-420:2021.
EVMinimumDischargeReactivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Rated minimum injected reactive power supported by the EV in vars. Corresponds to the EV.DSTO.DschAvarMinRtg attribute in IEC 61850-7-420:2021.
EVSessionTotalDischargeEnergyAvailable	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Total energy value, in Wh, that EV is allowed to provide during the entire V2G session. The value is independent from the V2X Cycling area. Once this value reaches the value of 0, the EV may block any attempt to discharge to protect the battery health. Corresponds to the EV.DEGEN.SuscRtg.DSTO.OutWh attribute in IEC 61850-7-420:2021.
EVInverterSwVersion	simpleType: evInverterSwVersionType	Optional String containing the software version of the inverter. Corresponds to the EV.DINV.PhyNam.swRev attribute in IEC 61850-7-420:2021.
EVInverterHwVersion	simpleType: evInverterHwVersionType	Optional String containing the hardware version of the inverter. Corresponds to the EV.DINV.PhyNam.hwRev attribute in IEC 61850-7-420:2021.
EVInverterManufacturer	simpleType: evInverterManufacturerType	Optional String containing the manufacturer of the inverter. Corresponds to the EV.DINV.PhyNam.vendor attribute in IEC 61850-7-420:2021.
EVInverterModel	simpleType: evInverterModelType	Optional String containing the model info of the inverter. Corresponds to the EV.DINV.PhyNam.model attribute in IEC 61850-7-420:2021.
EVInverterSerialNumber	simpleType: evInverterSerialNumberType	Optional String containing the serial number of the inverter. Corresponds to the EV.DINV.PhyNam.serNum attribute in IEC 61850-7-420:2021.

NOTE Parameter names ending with an asterisk (*) have additional optional elements for L2 and L3. Those parameters were omitted from this table for the sake of readability but are included in the schema.

L.2.2.1.3 DER_AC_CPDResEnergyTransferModeType

[V2G20-3149] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.6 and Figure L.6.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

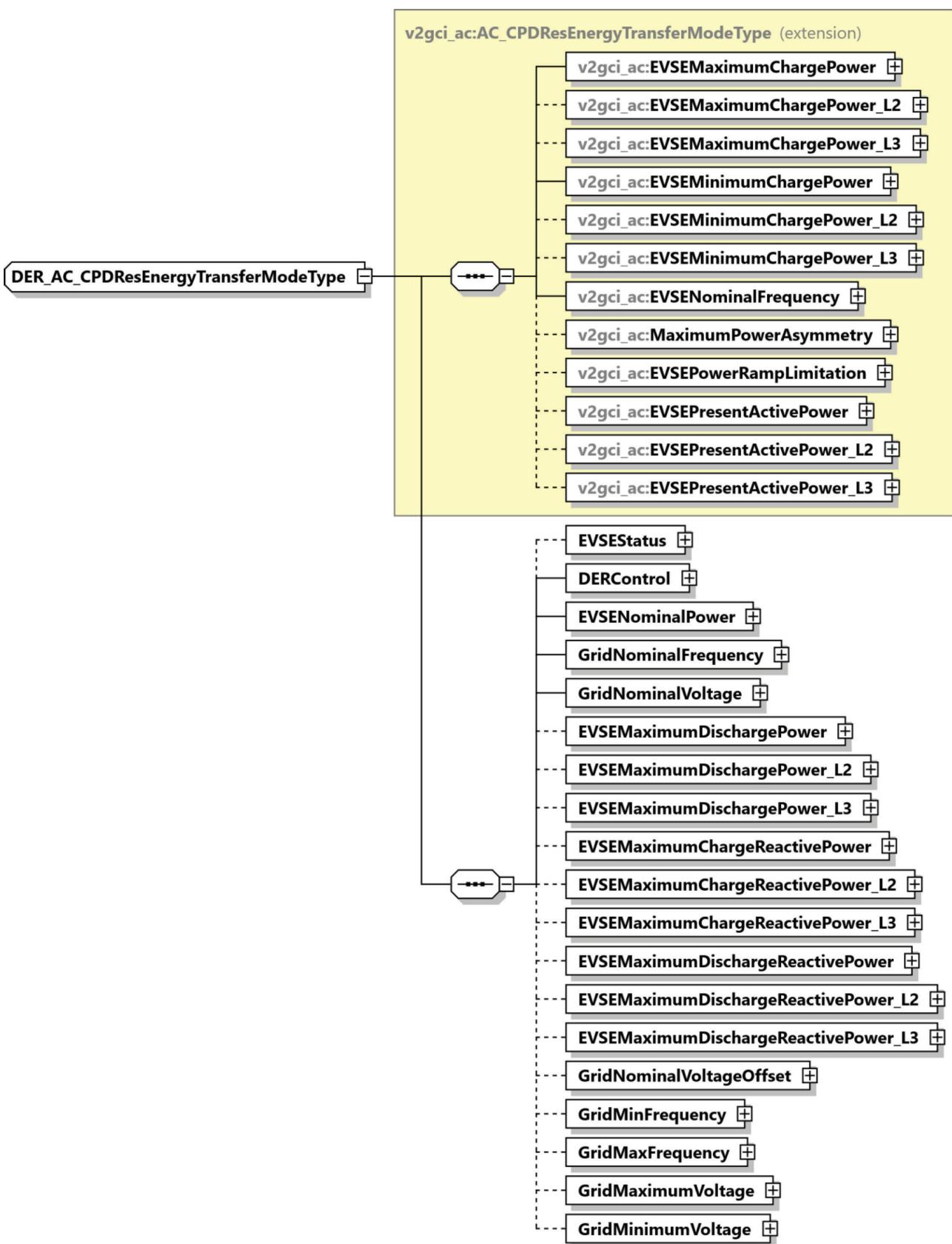


Figure L.6 — Schema diagram – `DER_AC_CPDResEnergyTransferModeType`

The elements of this message are used according to Table L.6.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table L.6 — Semantics and type definition for DER_AC_CPDResEnergyTransferModeType

ElementName	Type	Semantics
EVSEMaximumChargePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Mandatory Maximum absorbed active power supported by the EVSE and the site in watts. Corresponds to the EVSE.DSTO.ChaWMax attribute in IEC 61850-7-420:2021.
EVSEMinimumChargePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Mandatory Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts
EVSENominalFrequency	complexType: RationalNumberType refer to 8.3.5.3.8	Mandatory This is the nominal frequency supported by the EVSE.
MaximumPowerAsymmetry	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum asymmetric power in Watt. The maximal difference in Watt between any two of the up to three available phases.
EVSEPowerRampLimitation	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Limitation of the power variation in %/min
EVSEPresentActivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE. This value is based on the actual voltage and not the EVSENominalVoltage.
EVSEStatus	complexType: EVSEStatusType refer to 8.3.5.3.26	Optional: This element is used by the SECC for indicating the EVSE status and for signalling an event the SECC expects the EVCC to react to.
DERControl	complexType DERControlType refer to L.2.2.1.8	This contains all the functions related to the Grid Code that the EVSE sets the EV to run, respecting the DER functions the EV supports (reported via the DERControlFunctions attribute in the CPD Request). The settings may contain Voltage and Frequency Trip, Enter Service parameters, and Reactive and Active Power support methods.
EVSENominalPower	complexType: RationalNumberType refer to 8.3.5.3.8	Rated power of the EVSE in W. Corresponds to the EVSE.DSTO.WRtg attribute in IEC 61850-7-420:2021.
GridNominalFrequency	complexType: RationalNumberType refer to 8.3.5.3.8	This is the nominal working frequency of the grid where the EVSE is located (in Hz). Corresponds to the Grid.DPCC.HzNom attribute in IEC 61850-7-420:2021.
GridNominalVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Regular grid operation voltage (absolute value in V). Corresponds to the Grid.DPCC.VRef attribute in IEC 61850-7-420:2021. NOTE This corresponds to the voltage between L1 and neutral pins of the EV socket outlet or the vehicle connector.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table L.6 (continued)

ElementName	Type	Semantics
EVSEMaximumDischargePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Maximum injected active power supported by the EVSE and the site in watts. Corresponds to the EVSE.DSTO.DschWMax attribute in IEC 61850-7-420:2021.
EVSEMaximumChargeReactivePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Maximum absorbed reactive power supported by the EVSE and the site in vars. Corresponds to the EVSE.DSTO.ChaAvarMax attribute in IEC 61850-7-420:2021.
EVSEMaximumDischargeReactivePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Maximum injected reactive power supported by the EVSE and the site in vars. Corresponds to the EVSE.DSTO.DschIvarMax attribute in IEC 61850-7-420:2021.
GridNominalVoltageOffset	complexType: RationalNumberType refer to 8.3.5.3.8	Optional The nominal ac voltage (rms) offset between the DER's electrical connection point and the utility's point of common coupling present at the site.
GridMinFrequency	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Minimum grid permanent operation frequency possible (absolute value in Hz). Corresponds to the Grid.DPCC.HzNom.minVal attribute in IEC 61850-7-420:2021.
GridMaxFrequency	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Maximum grid permanent operation frequency possible (absolute value in Hz). Corresponds to the Grid.DPCC.HzNom.maxVal attribute in IEC 61850-7-420:2021.
GridMaximumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Maximum grid permanent operation voltage (absolute value in V). Corresponds to the Grid.DPCC.VMax attribute in IEC 61850-7-420:2021.
GridMinimumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Minimum grid permanent operation voltage (absolute value in V). Corresponds to the Grid.DPCC.VMin attribute in IEC 61850-7-420:2021.

NOTE 1 Parameter names ending with an asterisk (*) have additional optional elements for L2 and L3. Those parameters were omitted from this table for the sake of readability but are included in the schema.

[V2G20-3150] [DER] If the EVCC is not finished processing the parameters provided in the AC_DER_ChargeParameterDiscoveryRes, the EVCC shall send a AC_DER_ChargeParameterDiscoveryReq with EVProcessing set to "Ongoing" within V2G_EVCC_Sequence_Performance_Time according to Table 215.

[V2G20-3151] [DER] If the EVCC has finished processing the parameters provided in the AC_DER_ChargeParameterDiscoveryRes, the EVCC shall send a AC_DER_ChargeParameterDiscoveryReq with EVProcessing set to "Finished" within V2G_EVCC_Sequence_Performance_Time according to Table 215.

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

[V2G20-3152] [DER] The EVCC shall comply with the DER control parameters and settings that the SECC provides in the DERControl element.

[V2G20-3153] [DER] If the EVCC finds the settings provided by the SECC in the AC_DER_ChargeParameterDiscoveryRes to be inadequate and cannot accept them, the EVCC shall trigger a service renegotiation by sending a SessionStopReq with "ChargingSession" set to "ServiceRenegotiation".

[V2G20-3154] [DER] If the EVCC previously started a service renegotiation due to issues with the AC DER service, the EVCC should not select the AC DER service again during the current coupling session.

[V2G20-3155] [DER] If the AC DER service has been selected, the EVCC shall ignore the value of EVSE-NominalFrequency and instead use the value of GridNominalFrequency.

[V2G20-3156] [DER] If the AC DER service has been selected, the SECC shall not send the parameter EVSEPowerRampLimitation.

NOTE 2 If needed, the parameter PowerUpRamp will be used for hysteresis control.

[V2G20-3157] [DER] If the AC DER service has been selected, the SECC shall not send the parameter EVSEPresentActivePower.

[V2G20-3158] [DER] If the SECC needs to update the DER control parameters sent to the EVCC in the DERControl parameter in the AC_DER_ChargeParameterDiscoveryRes message, the SECC shall use the DERControl parameter in the AC_ChargeLoopRes.

[V2G20-3159] [DER] When a grid event occurs (e.g., over voltage, over frequency deviation), which triggers a reaction of the EV to support the grid, the EVCC shall use the field DERGridSupportActiveInfo in the AC_ChargeLoopReq to notify the SECC that the support has started, by setting the EventCondition field to '1'.

NOTE 3 For example, during reactive power support, the EV may not be able to discharge at full power to keep the minimal reactive power needed by the grid. In this case, it is relevant to get the info the EV is supporting the grid, so that the SECC can inform every business logic operator that the EV may not respect the agreed schedule or the targets dynamically set.

[V2G20-3160] [DER] Following **[V2G20-XX22] [DER]**, once the event is cleared and the grid is stabilized, the EVCC shall use the field DERGridSupportActiveInfo in the ChargeLoopReq, notifying the SECC that the initial disturbance has been resolved and the EV is now under normal operation, by setting the EventCondition field to '0' ("Ended").

[V2G20-3161] [DER] If EnterService is configured, when a grid event has occurred and it has been resolved, the EV may return to service, following the Enter Service settings.

[V2G20-3162] [DER] During the charging loop, the EVCC shall send the EV parameters considering the settings sent by the SECC with the AC_DER_ChargeParameterDiscoveryRes message and its own battery pack constraints (SoC, SoH, temperature, ...).

L.2.2.1.4 DER_Dynamic_AC_CLReqControlModeType

[V2G20-3163] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.7 and Figure L.7.

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Figure L.7 — Schema diagram – `DER_Dynamic_AC_CLReqControlModeType`**

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

The elements of this message are used according to Table L.7.

Table L.7 — Semantics and type definition for DER_Dynamic_AC_CLReqControlModeType

ElementName	Type	Semantics
DepartureTime	simpleType: xs:unsignedInt	Optional This element is used to indicate when the EV intends to finish the energy transfer process. The value is encoded in seconds since the TimeStamp of the message header (see [V2G20-2104]).
EVTargetEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	The energy request of the EV it needs to fulfil the target SOC as specified by the owner.
EVMaximumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Mandatory Maximum acceptable energy level of the EV
EVMinimumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Mandatory The energy request of the EV it needs to fulfil the minimum SOC as specified by the owner.
EVMaximumChargePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Mandatory EV momentary maximum absorbed active power supported by the EV at unity power factor. Corresponds to the EV.DSTO.ChaWMax attribute in IEC 61850-7-420:2021.
EVMinimumChargePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Mandatory EV momentary minimum absorbed active power supported by the EV at unity power factor. Corresponds to the EV.DSTO.ChaWMin attribute in IEC 61850-7-420:2021.
EVPresentActivePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Mandatory Present active power achieved by the EV
EVPresentReactivePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Mandatory Present reactive power achieved by the EV

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table L.7 (continued)

ElementName	Type	Semantics
EVOverExcitedMaximumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary maximum injected active power supported by the EV at specified over-excited power factor, given its current SoC, SoH, temperature, the limits imposed by the EVSE and other constraints. It can also be defined as the momentary EV maximum discharge power at the minimum injected reactive power value. This means that if the EV is providing reactive power support, and it is requested to discharge at max power (eg to satisfy an EMS request), the EV may override the request and discharge up to EVOverExcitedMaximumDischargePower to meet the minimum reactive power requirements. Corresponds to the EV.DSTO.DschWOvPF attribute in IEC 61850-7-420:2021.
EVOverExcitedPowerFactor	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV power factor when injecting (over excited) the minimum reactive power (EVMinimumDischargeReactivePower) Corresponds to the EV.DSTO.DschOvPFRtg attribute in IEC 61850-7-420:2021.
EVUnderExcitedMaximumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary maximum injected power supported by the EV at specified under-excited power factor, given its current SoC, SoH, temperature the limits imposed by the EVSE and other constraints. It can also be defined as the momentaneous EV maximum discharge power at the minimum absorbed reactive power value. This means that if the EV is providing reactive power support, and it is requested to discharge at max power (eg to satisfy an EMS request), the EV may override the request and discharge up to EVUnderExcitedMaximumDischargePower to meet the minimum reactive power requirements. Corresponds to the EV.DSTO.DschWUnPF attribute in IEC 61850-7-420:2021.
EVUnderExcitedPowerFactor	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV power factor when absorbing (under excited) the minimum reactive power (EVMinimumChargeReactivePower) Corresponds to the EV.DSTO.DschUnPFRtg attribute in IEC 61850-7-420:2021.
EVMaximumChargeApparentPower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary maximum absorbed apparent power supported by the EV in va. Corresponds to the EV.DSTO.ChaVAMax attribute in IEC 61850-7-420:2021.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table L.7 (continued)

ElementName	Type	Semantics
EVMaximumDischargeApparentPower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary injected apparent power supported by the EV in va. Corresponds to the EV.DSTO.DschVAMax attribute in IEC 61850-7-420:2021.
EVMaximumChargeReactivePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary maximum absorbed reactive power supported by the EV in vars. Corresponds to the EV.DSTO.ChaAvarMax attribute in IEC 61850-7-420:2021.
EVMaximumDischargePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Mandatory EV momentary maximum injected active power supported by the EV at unity power factor. EV.DSTO.DschWMax in IEC 61850-7-420:2021.
EVMinimumDischargePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Mandatory EV momentary minimum injected active power supported by the EV at unity power factor. Corresponds to the EV.DSTO.DschWMin attribute in IEC 61850-7-420:2021.
EVMinimumChargeReactivePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary minimum absorbed reactive power supported by the EV in vars. Corresponds to the EV.DSTO.ChaAvarMin attribute in IEC 61850-7-420:2021.
EVMaximumDischargeReactivePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary maximum injected reactive power supported by the EV in vars. Corresponds to the EV.DSTO.DschIvarMax attribute in IEC 61850-7-420:2021.
EVMinimumDischargeReactivePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary minimum injected reactive power supported by the EV in vars. Corresponds to the EV.DSTO.DschAvarMin attribute in IEC 61850-7-420:2021.
EVPresentVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV Present Voltage reading in V. Corresponds to the EV.MMXU.V attribute in IEC 61850-7-420:2021.
EVPresentFrequency	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV Present Frequency reading in Hz. Corresponds to the EV.MMXU.Hz attribute in IEC 61850-7-420:2021.
EVSetNominalVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Nominal AC rms voltage that the inverter is configured to. Corresponds to the EV.DECPVRef attribute in IEC 61850-7-420:2021.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table L.7 (continued)

ElementName	Type	Semantics
EVSetNominalVoltageOffset	complexType: RationalNumberType refer to 8.3.5.3.8	Optional The nominal ac voltage (rms) offset between the DER's electrical connection point and the utility's point of common coupling configured. This value shall be set by the EVCC to be equal to the GridNominalVoltageOffset. Corresponds to the EVSE.DECP.VOf attribute in IEC 61850-7-420:2021.
EVSetMaximumNominalVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Maximum AC rms voltage the inverter is set to operate with. Corresponds to the EV.DECP.VMax attribute in IEC 61850-7-420:2021.
EVSetMinimumNominalVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Minimum AC rms voltage the inverter is set to operate with. Corresponds to the EV.DECP.VMin attribute in IEC 61850-7-420:2021.
EVSessionTotalDischargeEnergyAvailable	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Total energy value, in Wh, that EV is allowed to provide during the entire V2G session. The value is independent from the V2X Cycling area. Once this value reaches the value of 0, the EV may block any attempt to discharge in order to protect the battery health. Corresponds to the EV.DSTO.OutWh attribute in IEC 61850-7-420:2021.
DERGridSupportActiveInfoType	complexType: DERGridSupport ActiveInfoType refer to L.2.2.1.28	Optional: Mandatory info to be reported by the EV when a grid event occurs or ceases to exist and that causes the EV to support or stop supporting the grid, respectively.

NOTE Parameter names ending with an asterisk ('*') have additional optional elements for L2 and L3. Those parameters were omitted from this table for the sake of readability but are included in the schema.

L.2.2.1.5 DER_Scheduled_AC_CLReqControlModeType

[V2G20-3164] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.8 and Figure L.8.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

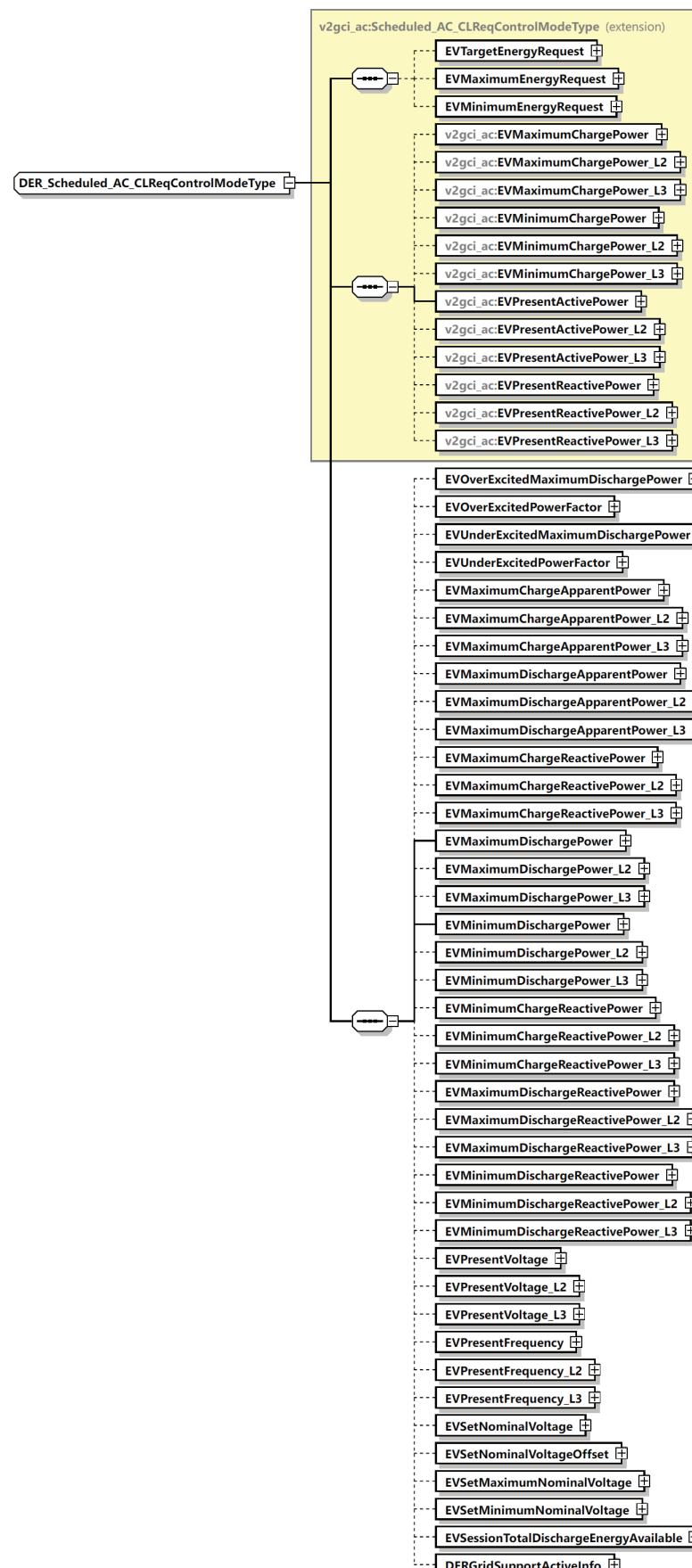


Figure L.8 — Schema diagram – `DER_Scheduled_AC_CLReqControlModeType`

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

The elements of this message are used according to Table L.8.

Table L.8 — Semantics and type definition for DER_Scheduled_AC_CLReqControlModeType

ElementName	Type	Semantics
EVTargetEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional The energy request of the EV it needs to fulfil the target SOC as specified by the owner.
EVMaximumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Maximum acceptable energy level of the EV
EVMinimumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional The energy request of the EV it needs to fulfil the minimum SOC as specified by the owner.
EVMaximumChargePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary maximum absorbed active power supported by the EV at unity power factor. Corresponds to the EV.DSTO.ChaWMax attribute in IEC 61850-7-420:2021.
EVMinimumChargePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary minimum absorbed active power supported by the EV at unity power factor. Corresponds to the EV.DSTO.ChaWMin attribute in IEC 61850-7-420:2021.
EVPresentActivePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Mandatory Present active power achieved by the EV
EVPresentReactivePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Present reactive power achieved by the EV
EVOVERExcitedMaximumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary maximum injected active power supported by the EV at specified over-excited power factor, given its current SoC, SoH, temperature, the limits imposed by the EVSE and other constraints. It can also be defined as the momentary EV maximum discharge power at the minimum injected reactive power value. This means that if the EV is providing reactive power support, and it is requested to discharge at max power (eg to satisfy an EMS request), the EV may override the request and discharge up to EVOVERExcitedMaximumDischargePower to meet the minimum reactive power requirements. Corresponds to the EV.DSTO.DschWOvPF attribute in IEC 61850-7-420:2021.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table L.8 (continued)

ElementName	Type	Semantics
EVOverExcitedPowerFactor	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV power factor when injecting (over excited) the minimum reactive power (EVMinimumDischargeReactivePower) Corresponds to the EV.DSTO.DschOvPFRtg attribute in IEC 61850-7-420:2021.
EVUnderExcitedMaximumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary maximum injected power supported by the EV at specified under-excited power factor, given its current SoC, SoH, temperature the limits imposed by the EVSE and other constraints. It can also be defined as the momentaneous EV maximum discharge power at the minimum absorbed reactive power value. This means that if the EV is providing reactive power support, and it is requested to discharge at max power (eg to satisfy an EMS request), the EV may override the request and discharge up to EVUnderExcitedMaximumDischargePower to meet the minimum reactive power requirements. Corresponds to the EV.DSTO.DschWUnPF attribute in IEC 61850-7-420:2021.
EVUnderExcitedPowerFactor	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV power factor when absorbing (under excited) the minimum reactive power (EVMinimumChargeReactivePower) Corresponds to the EV.DSTO.DschUnPFRtg attribute in IEC 61850-7-420:2021.
EVMaximumChargeApparentPower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary maximum absorbed apparent power supported by the EV in va. Corresponds to the EV.DSTO.ChaVAMax attribute in IEC 61850-7-420:2021.
EVMaximumDischargeApparentPower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary injected apparent power supported by the EV in va. Corresponds to the EV.DSTO.DschVAMax attribute in IEC 61850-7-420:2021.
EVMaximumChargeReactivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary maximum absorbed reactive power supported by the EV in vars. Corresponds to the EV.DSTO.ChaAvarMax attribute in IEC 61850-7-420:2021.
EVMaximumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary maximum injected active power supported by the EV at unity power factor. EV.DSTO.DschWMax in IEC 61850-7-420:2021.
EVMinimumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary minimum injected active power supported by the EV at unity power factor. Corresponds to the EV.DSTO.DschWMin attribute in IEC 61850-7-420:2021.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table L.8 (continued)

ElementName	Type	Semantics
EVMinimumChargeReactivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary minimum absorbed reactive power supported by the EV in vars. Corresponds to the EV.DSTO.ChaAvarMin attribute in IEC 61850-7-420:2021.
EVMaximumDischargeReactivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary maximum injected reactive power supported by the EV in vars. Corresponds to the EV.DSTO.DschIvarMax attribute in IEC 61850-7-420:2021.
EVMinimumDischargeReactivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV momentary minimum injected reactive power supported by the EV in vars. Corresponds to the EV.DSTO.DschAvarMin attribute in IEC 61850-7-420:2021.
EVPresentVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV Present Voltage reading in V. Corresponds to the EV.MMXU.V attribute in IEC 61850-7-420:2021.
EVPresentFrequency	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EV Present Frequency reading in Hz. Corresponds to the EV.MMXU.Hz attribute in IEC 61850-7-420:2021.
EVSetNominalVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Nominal AC rms voltage that the inverter is configured to. Corresponds to the EV.DECP.VRef attribute in IEC 61850-7-420:2021.
EVSetNominalVoltageOffset	complexType: RationalNumberType refer to 8.3.5.3.8	Optional The nominal ac voltage (rms) offset between the DER's electrical connection point and the utility's point of common coupling configured. This value shall be set by the EVCC to be equal to the GridNominalVoltageOffset. Corresponds to the EVSE.DECP.VOf attribute in IEC 61850-7-420:2021.
EVSetMaximumNominalVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Maximum AC rms voltage the inverter is set to operate with. Corresponds to the EV.DECP.VMax attribute in IEC 61850-7-420:2021.
EVSetMinimumNominalVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Minimum AC rms voltage the inverter is set to operate with. Corresponds to the EV.DECP.VMin attribute in IEC 61850-7-420:2021.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

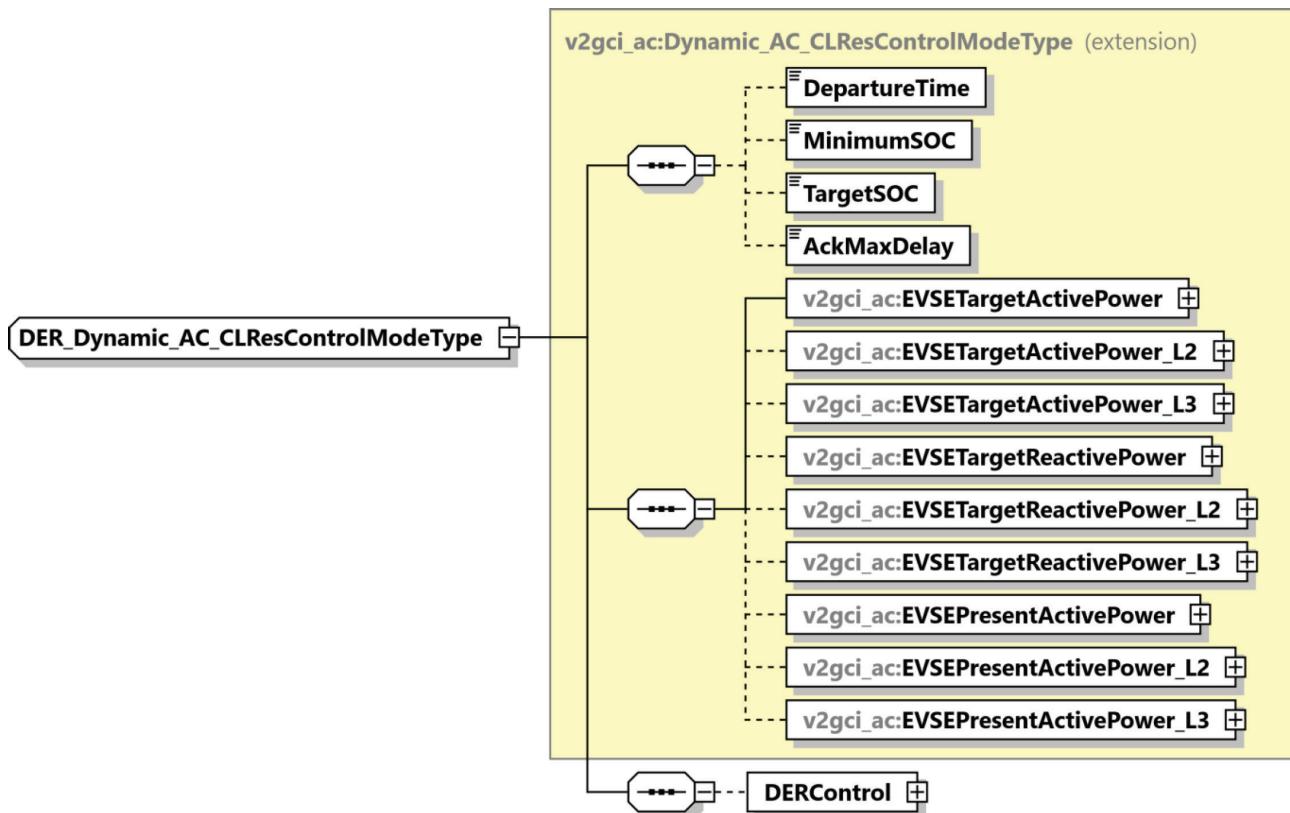
Table L.8 (continued)

ElementName	Type	Semantics
EVSessionTotalDischargeEnergyAvailable	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Total energy value, in Wh, that EV is allowed to provide during the entire V2G session. The value is independent from the V2X Cycling area. Once this value reaches the value of 0, the EV may block any attempt to discharge in order to protect the battery health. Corresponds to the EV.DSTO.OutWh attribute in IEC 61850-7-420:2021.
DERGridSupportActiveInfoType	complexType: DERGridSupport ActiveInfoType refer to L.2.2.1.28	Optional: Mandatory info to be reported by the EV when a grid event occurs or ceases to exist and that causes the EV to support or stop supporting the grid, respectively.

NOTE Parameter names ending with an asterisk ('*') have additional optional elements for L2 and L3. Those parameters were omitted from this table for the sake of readability but are included in the schema.

L.2.2.1.6 DER_Dynamic_AC_CLResControlModeType

[V2G20-3165] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.9 and Figure L.9.

**Figure L.9 — Schema diagram – DER_Dynamic_AC_CLResControlModeType**

The elements of this message are used according to Table L.9.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table L.9 — Semantics and type definition for DER_Dynamic_AC_CLResControlModeType

ElementName	Type	Semantics
DepartureTime	simpleType: xs:unsignedInt	This element is used to indicate when the EV intends to finish the energy transfer process. The value is encoded in seconds since the TimeStamp of the message header (see [V2G20-2104]).
MinimumSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: Minimum State of Charge EV needs to keep throughout the charging session. Mandatory when service parameter MobilityNeeds-Mode was set to 2
TargetSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: New TargetSOC value updated by the user from EVSE's side. Only used when service parameter MobilityNeeds-Mode was set to 2
AckMaxDelay	simpleType: xs:unsignedShort	Optional: This value indicates the maximum delay in seconds that SECC expects the EVCC to apply new mobility needs (DepartureTime or TargetSOC or MinimumSOC) and send updated values in a Charge Loop message since the reception of the message stating the AckMaxDelay.
EVSETargetActivePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Target active power requested by the EVSE
EVSETargetReactivePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target reactive power requested by the EVSE
EVSEPresentActivePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE. This value is based on the actual voltage and not the EVSENominalVoltage.
DERControl	complexType DERControlType refer to L.2.2.1.8	Optional: This contains all the functions related to the Grid Code that the EVSE mandates the EV to run, respecting the DER functions the EV supports (reported via the DERControlFunctions attribute in the CPD Request), The settings may contain Voltage and Frequency Trip, Enter Service parameters, and Reactive and Active Power support methods.

NOTE Parameter names ending with an asterisk ('*') have additional optional elements for L2 and L3. Those parameters were omitted from this table for the sake of readability but are included in the schema.

L.2.2.1.7 DER_Scheduled_AC_CLResControlModeType

[V2G20-3166] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.10 and Figure L.10.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

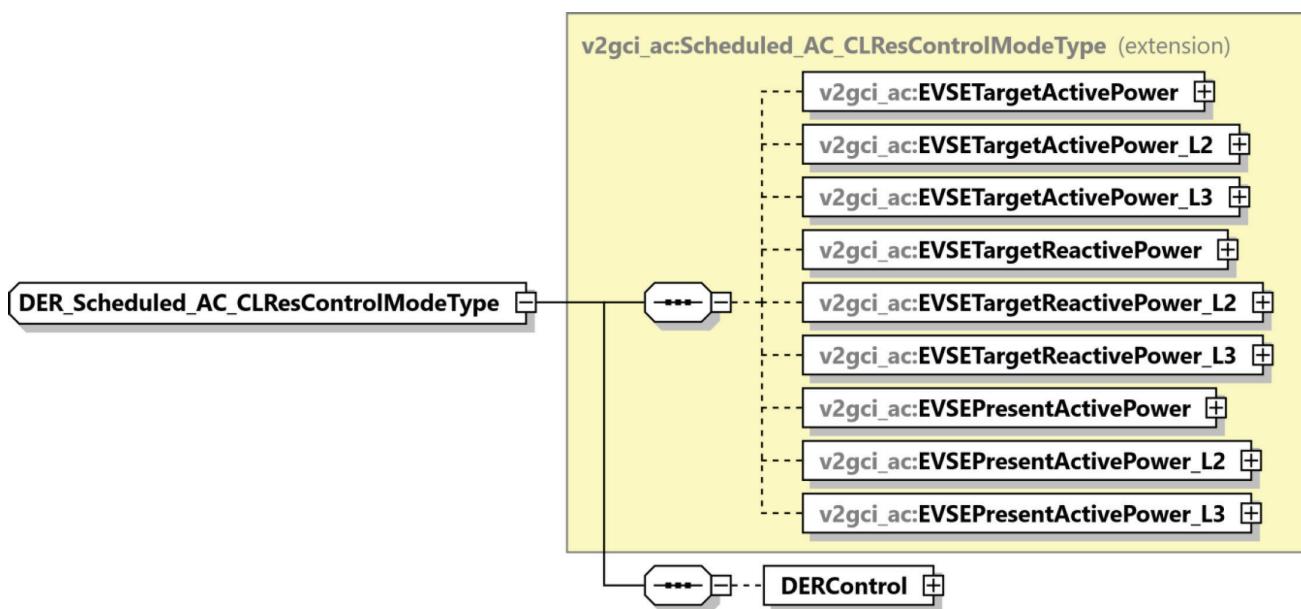


Figure L.10 — Schema diagram – DER_Scheduled_AC_CLResControlModeType

The elements of this message are used according to Table L.10.

Table L.10 — Semantics and type definition for DER_Scheduled_AC_CLResControlModeType

ElementName	Type	Semantics
EVSETargetActivePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target active power requested by the EVSE
EVSETargetReactivePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target reactive power requested by the EVSE
EVSEPresentActivePower*	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE. This value is based on the actual voltage and not the EVSENominalVoltage.
DERControl	complexType DERControlType refer to L.2.2.1.8	Optional: This contains all the functions related to the Grid Code that the EVSE mandates the EV to run, respecting the DER functions the EV supports (reported via the DERControlFunctions attribute in the CPD Request). The settings may contain Voltage and Frequency Trip, Enter Service parameters, and Reactive and Active Power support methods.

NOTE Parameter names ending with an asterisk (*) have additional optional elements for L2 and L3. Those parameters were omitted from this table for the sake of readability but are included in the schema.

L.2.2.1.8 DERControlType

[V2G20-3167] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.11 and Figure L.11.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

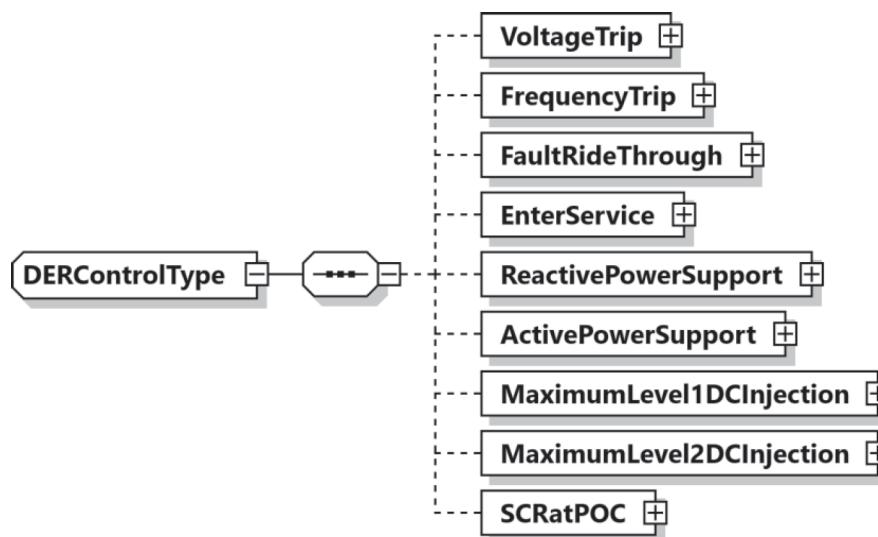


Figure L.11 — Schema diagram – DERControlType

The elements of this message are used according to Table L.11.

Table L.11 — Semantics and type definition for DERControlType

ElementName	Type	Semantics
VoltageTrip	complexType: VoltageTripType refer to L.2.2.1.11	Optional This element is used by the EVSE to inform the EV of the VoltageTrip parameters which apply in the region where the EVSE is installed. Only optional during CL.
FrequencyTrip	complexType: FrequencyTripType refer to L.2.2.1.12	Optional This element is used by the EVSE to inform the EV of the FrequencyTrip parameters which apply in the region where the EVSE is installed. Only optional during CL.
FaultRideThrough	complexType: FaultRideThroughType refer to L.2.2.1.9	Optional This element is used by the EVSE to inform the EV about the Fault-Ride-Through parameters which apply at the point of connection (POC)
EnterService	complexType: EnterServiceType refer to L.2.2.1.13	Optional Enter service after trip parameters
ReactivePowerSupport	complexType: ReactivePowerSupportType refer to L.2.2.1.14	Optional Contains the different Reactive Power Support methods/functions and its settings.
ActivePowerSupport	complexType: ActivePowerSupportType refer to L.2.2.1.15	Optional Contains the different Active Power Support methods/functions and its settings.

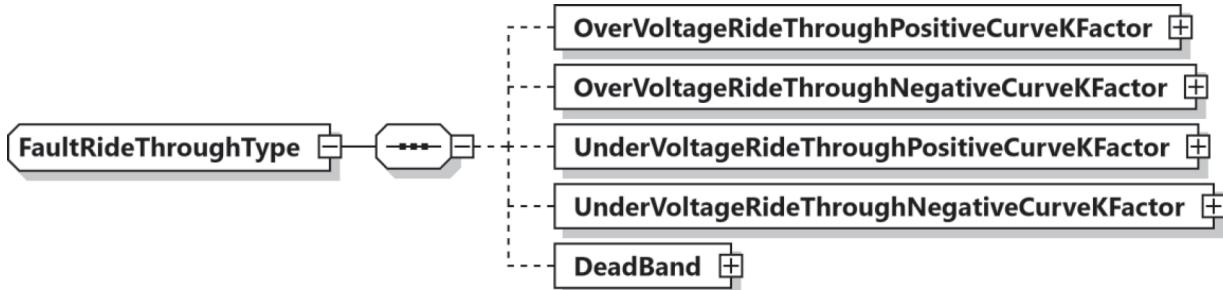
**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table L.11 (continued)

ElementName	Type	Semantics
MaximumLevel1DCInjection	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Unit: Amps Maximum injected DC current allowed at level 1 charging.
MaximumLevel2DCInjection	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Unit: Amps Maximum injected DC current allowed at level 2 charging. This element is only optional if restrictions to DC Injection do not apply.
SCRatPOC	complexType: RationalNumberType refer to 8.3.5.3.8	Optional It is the ratio of the short circuit apparent power in the case of a line-ground fault at the point of connection to the nominal power rating of the inverter itself. This element is not optional if Short Circuit Ratio bit is set to '1' in the DERExtendedControlFunctionsBitmap

L.2.2.1.9 FaultRideThroughType

[V2G20-3168] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.12 and Figure L.12.

**Figure L.12 — Schema diagram – FaultRideThroughType**

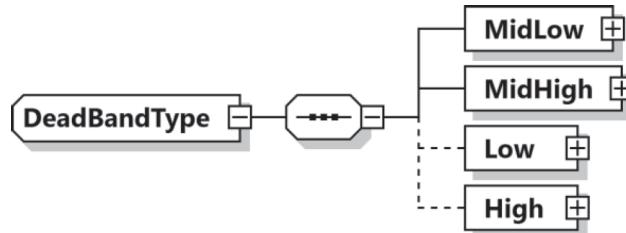
The elements of this message are used according to Table L.12.

Table L.12 — Semantics and type definition for FaultRideThroughType

ElementName	Type	Semantics
OverVoltageRideThroughPositiveCurveKFactor	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Over Voltage Positive sequence curve K factor Mandatory when bit 4 of the DERExtendedControlFunctions is enabled
OverVoltageRideThroughNegativeCurveKFactor	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Over Voltage Negative sequence curve K factor. Mandatory when bit 4 of the DERExtendedControlFunctions is enabled.
UnderVoltageRideThroughPositiveCurveKFactor	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Under Voltage Positive sequence curve K factor. Mandatory when bit 5 of the DERExtendedControlFunctions is enabled.
UnderVoltageRideThroughNegativeCurveKFactor	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Under Voltage Negative sequence curve K factor Mandatory when bit 5 of the DERExtendedControlFunctions is enabled.
DeadBand	complexType: DeadBandType refer to L.2.2.1.10	Voltage range bands to be used together with ZeroCurrent-Mode support or UVRT/OVRT support

L.2.2.1.10 DeadBandType

[V2G20-3169] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.13 and Figure L.13.

**Figure L.13 — Schema diagram – DeadBandType**

The elements of this message are used according to Table L.13.

Table L.13 — Semantics and type definition for DeadBandType

ElementName	Type	Semantics
MidLow	complexType: RationalNumberType refer to 8.3.5.3.8	Unit: Percentage Voltage middle lower limit for the dead band in percentage of the GridNominalVoltage.
MidHigh	complexType: RationalNumberType refer to 8.3.5.3.8	Unit: Percentage Voltage middle upper limit for the dead band in percentage of the GridNominalVoltage.
Low	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Unit: Percentage Voltage lower limit for the dead band in percentage of the GridNominalVoltage.
High	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Unit: Percentage Voltage upper limit for the dead band in percentage of the GridNominalVoltage.

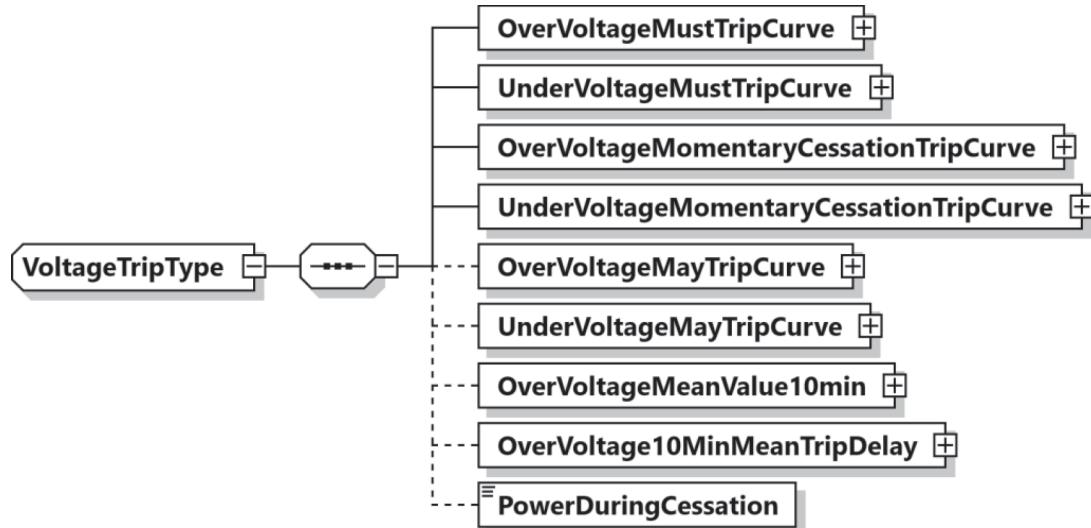
L.2.2.1.11 VoltageTripType

The Over/Under Voltage Ride-Through Must Trip, May Trip and Momentary Cessation Trip curves are specified by duration-volt curves that define the operating region under high or low-voltage conditions. Each curve is specified by an array of duration-volt pairs that will be interpolated into a piecewise linear function that defines an operating region. The x value of each pair specifies a duration (time at a given voltage in seconds).

The y value of each pair specifies an effective percentage voltage of the grid nominal voltage, defined as:

$$100 \% \times (\text{locally measured voltage} - \text{GridNominalVoltageOffset}) / \text{GridNominalVoltage}$$

[V2G20-3170] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.14 and Figure L.14.

**Figure L.14 — Schema diagram – VoltageTripType**

The elements of this message are used according to Table L.14.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**
Table L.14 — Semantics and type definition for VoltageTripType

ElementName	Type	Semantics
OverVoltageMustTripCurve	complexType: DERCurveType refer to L.2.2.1.18	Over Voltage Must Trip Curve This control specifies the “must trip region”.
UnderVoltageMustTripCurve	complexType: DERCurveType refer to L.2.2.1.18	Under Voltage Must Trip Curve This control specifies the “must trip region”.
OverVoltageMomentaryCessa-tionTripCurve	complexType: DERCurveType refer to L.2.2.1.18	Over Voltage Momentary Cessation Trip Curve This control specifies the “momentary cessation region”.
UnderVoltageMomentaryCessa-tionTripCurve	complexType: DERCurveType refer to L.2.2.1.18	Under Voltage Momentary Cessation Trip Curve This control specifies the “momentary cessation region”.
OverVoltageMayTripCurve	complexType: DERCurveType refer to L.2.2.1.18	Optional Over Voltage May Trip Curve This control specifies the “may trip region”.
UnderVoltageMayTripCurve	complexType: DERCurveType refer to L.2.2.1.18	Optional Under Voltage May Trip Curve This control specifies the “may trip region”.
OverVoltageMeanValue10min	complexType: RationalNumberType refer to 8.3.5.3.8	Optional EN 50549-1 chapter 4.9.3.4 Voltage threshold for the 10 min time window mean value monitoring. The 10 min mean is recalculated up to every 3 s. If the present voltage is above this threshold for more than the time defined by OverVoltage10Mi-nMeanTripDelay, the EV shall trip. This value is mandatory if OverVoltage10Mi-nMeanTripDelay is set
OverVoltage10MinMeanTripDe-lay	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Time for which the voltage is allowed to stay above the 10 min mean value. After this time, the EV shall trip. This value is mandatory if OverVoltageMeanValue-10min is set
PowerDuringCessation	simpleType: powerDuringCessationType enumeration refer to L.2.2.2.4	Optional Parameter is only sent, if the EV has to feed-in power or reactive power during fault-ride through (FRT) as defined by OverVoltage-MomentaryCes-sationTripCurve and UnderVoltage-Momentary-CessationTripCurve.

L.2.2.1.12 FrequencyTripType

The Over/Under Frequency Ride-Through Must Trip and May Trip curves are specified by a duration-frequency curve that defines the operating region of over/under-frequency conditions. Each curve is specified by an array of duration-frequency pairs that will be interpolated into a piecewise linear function that defines an operating region. The x value of each pair specifies a duration (time at a given frequency in seconds). The y value of each pair specifies a frequency, in hertz. The Rate of Change of Frequency (ROCOF) Trip Threshold is defined in Hertz/s.

[V2G20-3171] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.15 and Figure L.15.

- Entwurf -

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

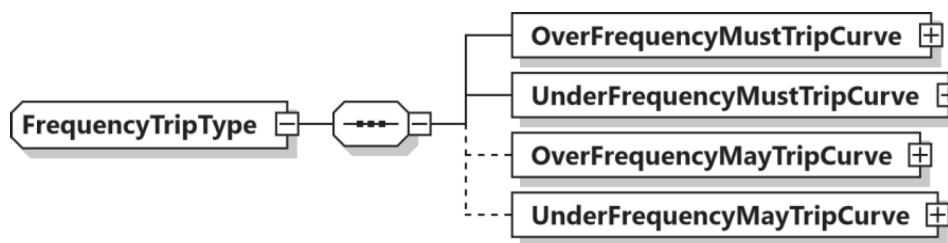


Figure L.15 — Schema diagram – FrequencyTripType

The elements of this message are used according to Table L.15.

Table L.15 — Semantics and type definition for FrequencyTripType

ElementName	Type	Semantics
OverFrequencyMustTripCurve	complexType: DERCurveType refer to L.2.2.1.18	Over Frequency Must Trip Curve This control specifies the “must trip region”.
UnderFrequencyMustTripCurve	complexType: DERCurveType refer to L.2.2.1.18	Under Frequency Must Trip Curve This control specifies the “must trip region”.
OverFrequencyMayTripCurve	complexType: DERCurveType refer to L.2.2.1.18	Optional Over Frequency May Trip Curve This control specifies the “may trip region”.
UnderFrequencyMayTripCurve	complexType: DERCurveType refer to L.2.2.1.18	Optional Under Frequency May Trip Curve This control specifies the “may trip region”.

L.2.2.1.13 EnterServiceType

[V2G20-3172] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.16 and Figure L.16.

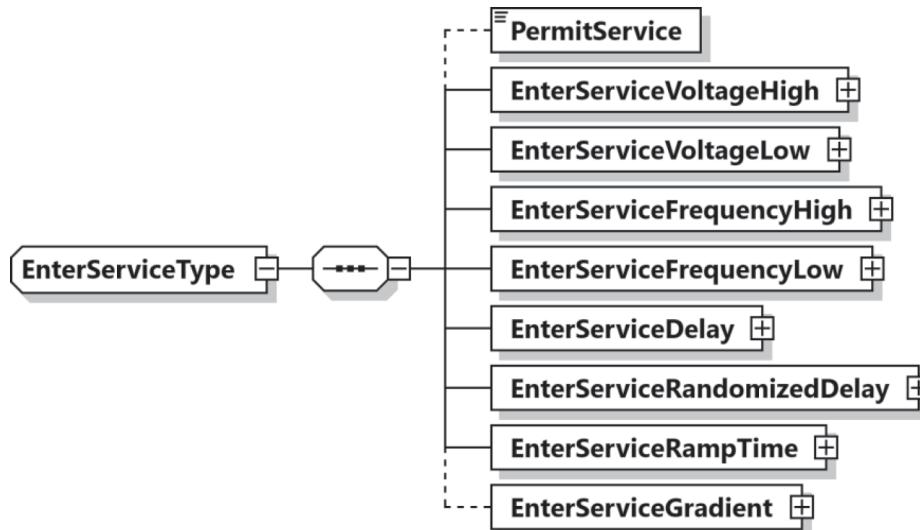


Figure L.16 — Schema diagram – EnterServiceType

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

The elements of this message are used according to Table L.16.

Table L.16 — Semantics and type definition for EnterServiceType

ElementName	Type	Semantics
PermitService	SimpleType: xs:boolean	Optional Flag to dictate if the EV is allowed to feedback energy to the grid. This parameter when set to false ("0") overrules any EVSE request to discharge. This field is introduced so compliance with IEEE 1547, section 10.6.10 is guaranteed. Corresponds to the EV.DGEN.PrmConn attribute in IEC 61850.
EnterServiceVoltageHigh	complexType: RationalNumberType refer to 8.3.5.3.8	High voltage value for enter service defined as an effective percent voltage of the GridNominalVoltage, according to the formula: $100 \times (\text{Voltage} - \text{GridNominalVoltageOffset}) / \text{GridNominalVoltage}$ Corresponds to the EV.DCTE.VHiLim attribute in IEC 61850-7-420:2021.
EnterServiceVoltageLow	complexType: RationalNumberType refer to 8.3.5.3.8	Low voltage value for enter service defined as an effective percent voltage of the GridNominalVoltage, according to the formula: $100 \times (\text{Voltage} - \text{GridNominalVoltageOffset}) / \text{GridNominalVoltage}$ Corresponds to the EV.DCTE.VLoLim attribute in IEC 61850-7-420:2021.
EnterServiceFrequencyHigh	complexType: RationalNumberType refer to 8.3.5.3.8	High frequency value for enter service, in absolute value. Corresponds to the EV.DCTE.HzHiLim attribute in IEC 61850-7-420:2021.
EnterServiceFrequencyLow	complexType: RationalNumberType refer to 8.3.5.3.8	Low frequency value for enter service, in absolute value. Corresponds to the EV.DCTE.HzLoLim attribute in IEC 61850-7-420:2021.
EnterServiceDelay	complexType: RationalNumberType refer to 8.3.5.3.8	Delay in seconds, for the EV to return to service after a grid event. Corresponds to the EV.DCTE.RtnDlTmms attribute in IEC 61850-7-420:2021.

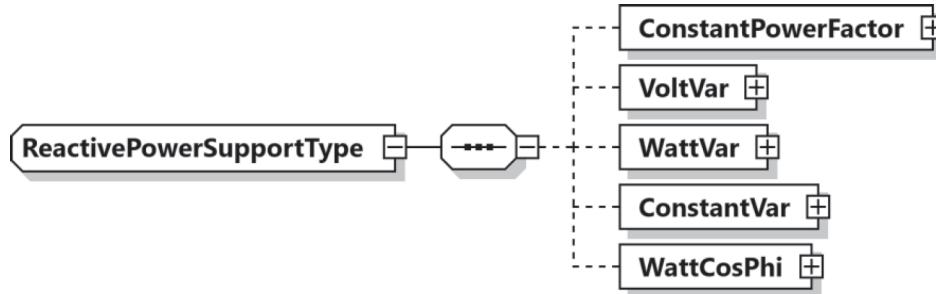
**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table L.16 (continued)

ElementName	Type	Semantics
EnterServiceRandomizedDelay	complexType: RationalNumberType refer to 8.3.5.3.8	Random value to add to the EnterServiceDelay. Corresponds to the EV.DCTE.WinTms attribute in IEC 61850-7-420:2021.
EnterServiceRampTime	complexType: RationalNumberType refer to 8.3.5.3.8	Enter service ramp rate in seconds. This is mandatory as it is important to even out the amount of power that is provided to avoid potential power peaks. Corresponds to the EV.DCTE.RtnRmpTmms attribute in IEC 61850-7-420:2021.
EnterServiceGradient	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Set default rate of change (ramp rate) of active power output due to command or internal action, defined in PercentageMaximumConfiguredDischargePower/second. Resolution is in hundreds of a percent/second. A value of 0 means there is no limit. Interpreted as a percentage change in output capability limit per second when used as a default ramp rate. PercentageMaximumConfiguredDischargePower = min(EVSEMaximumDischargePower, EVMaximumDischargePower). Corresponds to the EV.DCTE.RpuChaRteMax attribute in IEC 61850-7-420:2021.

L.2.2.1.14 ReactivePowerSupportType

[V2G20-3173] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.17 and Figure L.17.

**Figure L.17 — Schema diagram – ReactivePowerSupportType**

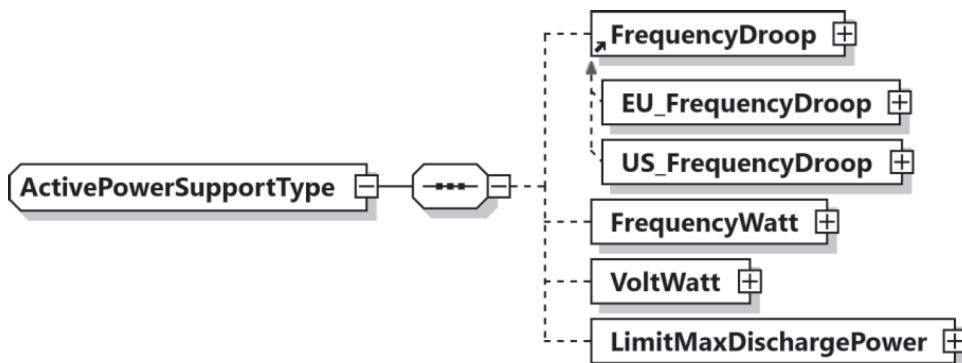
The elements of this message are used according to Table L.17.

Table L.17 — Semantics and type definition for ReactivePowerSupportType

ElementName	Type	Semantics
ConstantPowerFactor	complexType: ConstantPowerFactorType	Optional Constant Power factor Method. If no other Reactive Power Support method is used, then this one shall be filled
VoltVar	complexType: DERCurveType refer to L.2.2.1.18	Optional Volt-Var method. The static volt-var function provides over- or under-excited Var compensation as a function of measured voltage. The volt-var curve is specified as an array of volt-var pairs that are interpolated into a piecewise linear function. Corresponds to the EV.DVVR.VVArCrv attribute in IEC 61850-7-420:2021.
WattVar	complexType: DERCurveType refer to L.2.2.1.18	Optional Watt-Var method. The Watt-Var function varies vars as a function of delivered active power. The Watt-Var curve is specified as an array of Watt-Var pairs that are interpolated into a piecewise linear function with hysteresis. Corresponds to the EV.DWVR.WVArCrv attribute in IEC 61850-7-420:2021.
ConstantVar	complexType: ConstantVarType refer to L.2.2.1.17	Optional Sets a constant reactive power setpoint. Corresponds to the EV.DSTO.VArTgtSpt attribute in IEC 61850-7-420:2021.
WattCosPhi	complexType: DERCurveType refer to L.2.2.1.18	Optional The Watt-CosPhi function varies Cosine Phi as a function of delivered active power. The Watt-CosinePhi curve is specified as an array of Watt-CosPhi coordinates that are interpolated into a piecewise linear function with hysteresis. CosinePhi is a signed value and shall be interpreted in accordance with the standard used in the jurisdiction where the EV will be connected.

L.2.2.1.15 ActivePowerSupportType

[V2G20-3174] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.18 and Figure L.18.

**Figure L.18 — Schema diagram – ActivePowerSupportType**

The elements of this message are used according to Table L.18.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table L.18 — Semantics and type definition for ActivePowerSupportType

ElementName	Type	Semantics
EU_FrequencyDroop	complexType: EU_FrequencyDroopType refer to L.2.2.1.22	Optional Parametrized Frequency Droop setting for Active Power support, according to the EU convention, as defined by EN 50549. Mandatory when bit 2 of the DERExtendedControlFunction is set.
US_FrequencyDroop	complexType: US_FrequencyDroopType refer to L.2.2.1.24	Optional Parametrized Frequency Droop setting for Active Power support, according to the US convention, as defined by IEEE 1547. Mandatory when bit 8 of the DERStandardControlFunction is set.
FrequencyWatt	complexType: FrequencyWattCurveType refer to L.2.2.1.21	Optional The Frequency-Watt function limits active power generation or consumption when the line frequency deviates from nominal by a specified amount. The frequency-watt curve is specified as an array of frequency-watt pairs that are interpolated into a piecewise linear function. The x value of each pair specifies the frequency in Hertz. The y value specifies a corresponding active power output either in Watts or in “PercentageMaximumConfiguredDischargePower” or “PercentageMaximumConfiguredChargePower” as defined in curveDataPointsUnitType. This function can also contain an hysteresis window Corresponds to the EV.DHFW.HzWCrV attribute in IEC 61850-7-420:2021.
VoltWatt	complexType: DERCurveType refer to L.2.2.1.18	Optional The Volt-Watt curve limits maximum active power output or input as a function of measured voltage. The Volt-Watt curve is specified as an array of Volt-Watt pairs that are interpolated into a piecewise linear function. Corresponds to the EV.DVWC.VWCrV attribute in IEC 61850-7-420:2021.
LimitMaxDischargePower	complexType: LimitMaxDischargePowerType refer to L.2.2.1.27	Optional Limits the maximum active power that the EV can discharge. The value is set as a percentage of the rated EVMaximumDischargePower, reported during ChargeParameterDiscovery. Corresponds to the EV.DWMN.WLimPct attribute in IEC 61850-7-420:2021.

L.2.2.1.16 ConstantPowerFactorType

[V2G20-3175] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.19 and Figure L.19.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

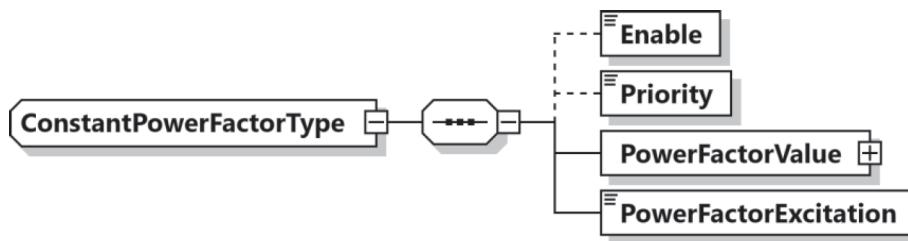


Figure L.19 — Schema diagram – ConstantPowerFactorType

The elements of this message are used according to Table L.19.

Table L.19 — Semantics and type definition for ConstantPowerFactorType

ElementName	Type	Semantics
Enable	simpleType: xs:boolean	Optional Enables the function if set to TRUE. Corresponds to the DFPF.Mod attribute in IEC 61850-7-420:2021.
Priority	simpleType: xs:unsignedShort	Optional Defines the priority of this function in respect to others. Priority = 0 is the highest. Corresponds to the DFPF.ModPrio attribute in IEC 61850-7-420:2021.
PowerFactorValue	complexType: RationalNumberType refer to 8.3.5.3.8	Power factor value between 0.0 and 1.0. Corresponds to the DFPF.PFGnTgt attribute in IEC 61850-7-420:2021.
PowerFactorExcitation	simpleType: PowerFactorExcitationType enumeration refer to L.2.2.2.5	Excitation type: Over-Excited (Injection) or Under-Excited (Absorption). Corresponds to the DFPF.PFGnExtQud attribute in IEC 61850-7-420:2021.

L.2.2.1.17 ConstantVarType

[V2G20-3176] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.20 and Figure L.20.

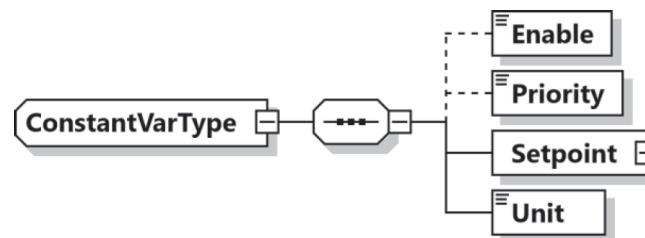


Figure L.20 — Schema diagram – ConstantVarType

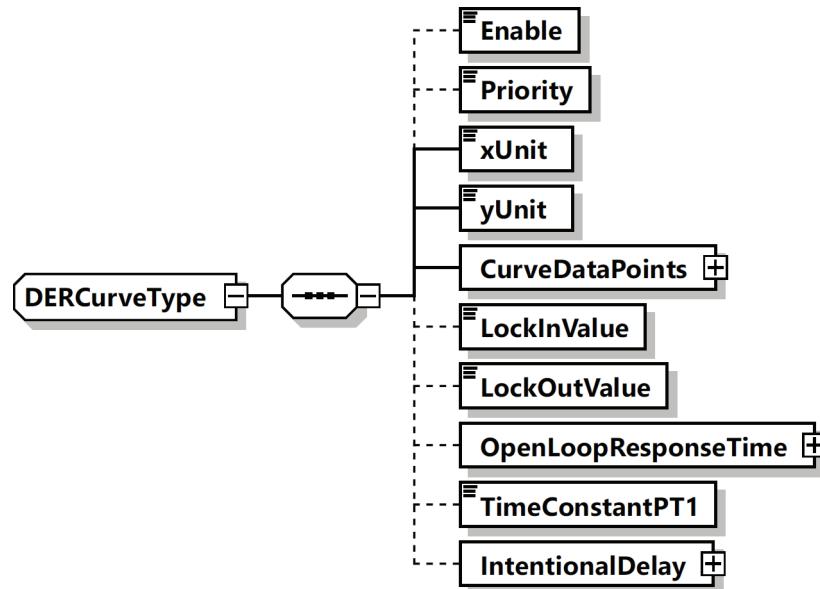
The elements of this message are used according to Table L.20.

Table L.20 — Semantics and type definition for ConstantVarType

ElementName	Type	Semantics
Enable	simpleType: xs:boolean	Optional: Enables the function if set to TRUE. Corresponds to the DVAR.Mod attribute in IEC 61850-7-420:2021.
Priority	simpleType: xs:unsignedShort	Optional Defines the priority of this function in respect to others. Priority = 0 is the highest. Corresponds to the DVAR.ModPrio attribute in IEC 61850-7-420:2021.
Setpoint	complexType: RationalNumberType refer to 8.3.5.3.8	The value specifies a target var output interpreted as a signed percentage (-100 to 100). A negative value refers to charging, whereas a positive one refers to discharging. The value type is determined by the Unit field. Corresponds to the EV.DWMN.DVAR.VArTgtPct attribute in IEC 61850-7-420:2021.
Unit	simpleType: curveDataPointsUnitType enumeration refer to L.2.2.2.1	One of “PercentageMaximumConfiguredDischargePower”, “PercentMaxConfiguredDischargeReactivePower” or “PercentMaxAvailableDischargeReactivePower”. Corresponds to the DVAR.VArSptRef attribute in IEC 61850-7-420:2021.

L.2.2.1.18 DERCurveType

[V2G20-3177] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.21 and Figure L.21.

**Figure L.21 — Schema diagram – DERCurveType**

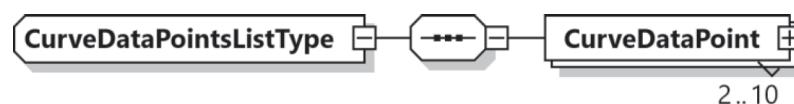
The elements of this message are used according to Table L.21.

Table L.21 — Semantics and type definition for DERCurveType

ElementName	Type	Semantics
Enable	simpleType: xs:boolean	Optional Enables the function if set to TRUE.
Priority	simpleType: xs:unsignedShort	Optional Defines the priority of this function in respect to others. Priority = 0 is the highest.
xUnit	simpleType: curveDataPointsUnitType enumeration refer to L.2.2.2.1	Data unit of the abscissa values
yUnit	simpleType: curveDataPointsUnitType enumeration refer to L.2.2.2.1	Data unit of the ordinate values
CurveDataPoints	complexType: CurveDataPointsListType refer to L.2.2.1.19	List of the data points (abscissa and ordinate) that together describe the curve.
LockInValue	simpleType: lockValueUnitType enumeration refer to L.2.2.2.7	Optional Absolute value e.g. power or voltage at which active/reactive control function shall be activated/locked-in.
LockOutValue	simpleType: lockValueUnitType enumeration refer to L.2.2.2.7	Optional Absolute value e.g. power or voltage at which active/reactive control function shall be deactivated/locked-out.
OpenLoopResponseTime	complexType: RationalNumberType refer to 8.3.5.3.8	Optional It is the time to ramp up to 90 % of the new target in response to the change in frequency. Corresponds to the DXXX.OplTmsMax attribute in IEC 61850-7-420:2021.
TimeConstantPT1	simpleType: xs:unsignedInt	Optional Unit: seconds Time constant to be applied to a PT1 response curve behaviour
IntentionalDelay	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Unit: seconds Delay before activating the control function

L.2.2.1.19 CurveDataPointsListType

[V2G20-3178] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.22 and Figure L.22.

**Figure L.22 — Schema diagram – CurveDataPointsListType**

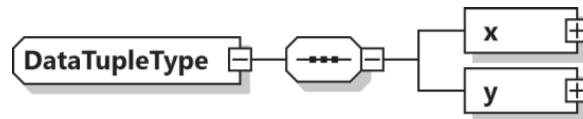
The elements of this message are used according to Table L.22.

Table L.22 — Semantics and type definition for CurveDataPointsListType

ElementName	Type	Semantics
CurveDataPoint	complexType: DataTupleType refer to L.2.2.1.20	Data tuple The curveDataPointsList has a minimum of 2 data tuples and a maximum of 10 data tuples

L.2.2.1.20 DataTupleType

[V2G20-3179] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.23 and Figure L.23.

**Figure L.23 — Schema diagram – DataTupleType**

The elements of this message are used according to Table L.23.

Table L.23 — Semantics and type definition for DataTupleType

ElementName	Type	Semantics
x	complexType: RationalNumberType refer to 8.3.5.3.8	Value for the X axis
y	complexType: RationalNumberType refer to 8.3.5.3.8	Value for the Y axis

L.2.2.1.21 FrequencyWattCurveType

[V2G20-3180] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.24 and Figure L.24.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

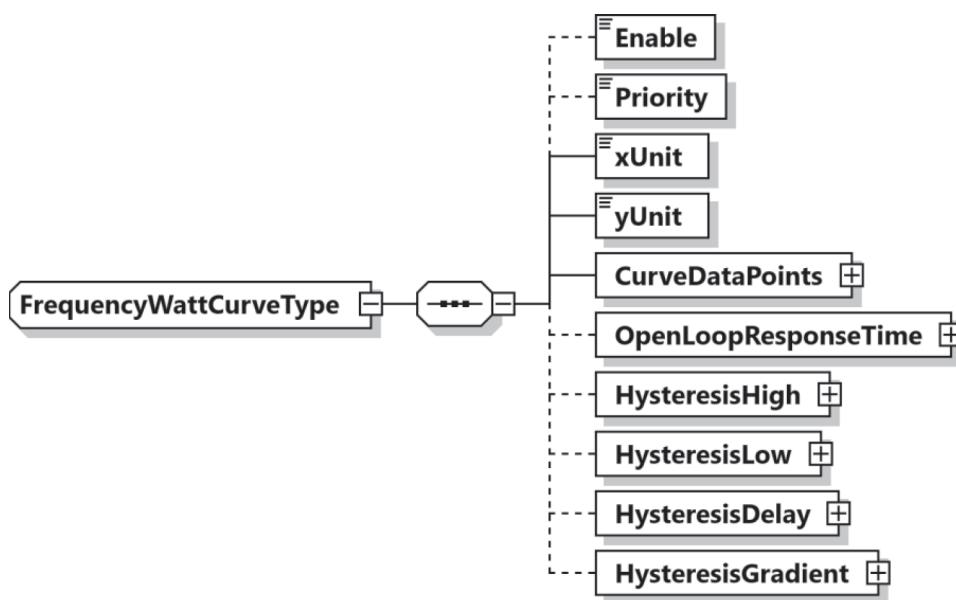


Figure L.24 — Schema diagram – FrequencyWattCurveType

The elements of this message are used according to Table L.24.

Table L.24 — Semantics and type definition for FrequencyWattCurveType

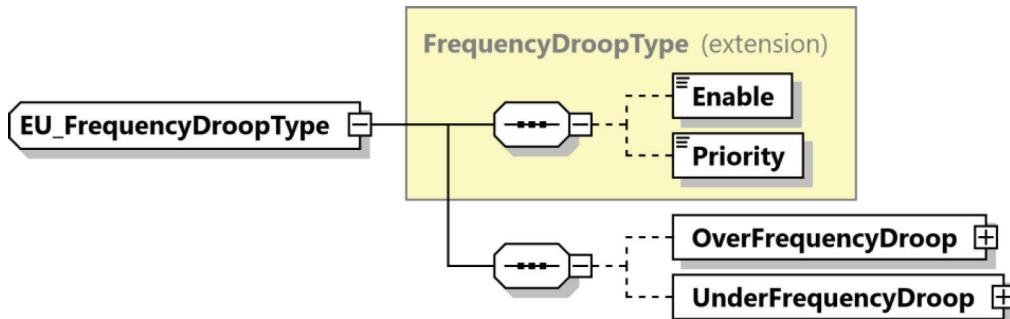
ElementName	Type	Semantics
Enable	simpleType: xs:boolean	Optional Enables the function if set to TRUE.
Priority	simpleType: xs:unsignedShort	Optional Defines the priority of this function in respect to others. Priority = 0 is the highest.
xUnit	simpleType: curveDataPointsUnitType enumeration refer to L.2.2.2.1	Data unit of the abscissa values
yUnit	simpleType: curveDataPointsUnitType enumeration refer to L.2.2.2.1	Data unit of the ordinate values
CurveDataPoints	complexType: CurveDataPointsListType refer to L.2.2.1.19	List of the data points (abscissa and ordinate) that together describe the curve.
OpenLoopResponseTime	complexType: RationalNumberType refer to 8.3.5.3.8	Optional It is the time to ramp up to 90 % of the new target in response to the change in frequency. Corresponds to the DXXX.OplTmsMax attribute in IEC 61850-7-420:2021.
HysteresisHigh	complexType: RationalNumberType refer to 8.3.5.3.8	Optional High value for return to normal operation after a grid event, in absolute value. This value adopts the same unit as defined by yUnit. Corresponds to the DHFW.HysCrv attribute in IEC 61850-7-420:2021.

Table L.24 (continued)

ElementName	Type	Semantics
HysteresisLow	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Low value for return to normal operation after a grid event, in absolute value. This value adopts the same unit as defined by yUnit. Corresponds to the DLFW.HysCrv attribute in IEC 61850-7-420:2021.
HysteresisDelay	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Delay in seconds, once grid parameter within HysteresisLow and HysteresisHigh, for the EV to return to normal operation after a grid event. Corresponds to the DHFW.ActStrDtTmms attribute in IEC 61850-7-420:2021.
HysteresisGradient	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Set default rate of change (ramp rate %/s) for the EV to return to normal operation after a grid event. Corresponds to the DHFW.HysGra attribute in IEC 61850-7-420:2021.

L.2.2.1.22 EU_FrequencyDroopType

[V2G20-3181] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.25 and Figure L.25.

**Figure L.25 — Schema diagram – EU_FrequencyDroopType**

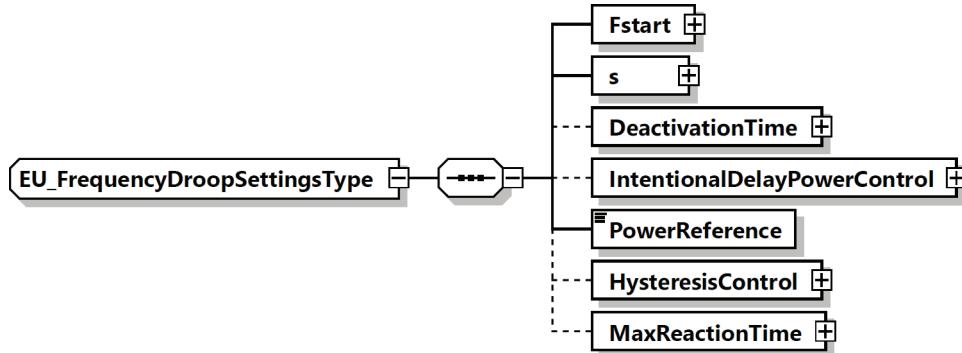
The elements of this message are used according to Table L.25.

Table L.25 — Semantics and type definition for EU_FrequencyDroopType

ElementName	Type	Semantics
Enable	SimpleType: xs:boolean	Optional Enables the function if set to TRUE. Corresponds to the DHFW.Mod and DLFW.Mod attribute in IEC 61850-7-420:2021.
Priority	SimpleType: xs:unsignedShort	Optional Defines the priority of this function in respect to others. Priority = 0 is the highest.
OverFrequencyDroop	complexType: EU_FrequencyDroopSettingsType refer to L.2.2.1.23	Optional Values for the Over Frequency Droop curve. If this field is not present, then the UnderFrequencyDroop shall be provided. Corresponds to the DHFW.HzWCrv attribute in IEC 61850-7-420:2021.
UnderFrequencyDroop	complexType: EU_FrequencyDroopSettingsType refer to L.2.2.1.23	Optional Values for the Under Frequency Droop curve. If this field is not present, then the OverFrequencyDroop shall be provided. Corresponds to the DLFW.HzWCrv attribute in IEC 61850-7-420:2021.

L.2.2.1.23 EU_FrequencyDroopSettingsType

[V2G20-3182] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.26 and Figure L.26.

**Figure L.26 — Schema diagram – EU_FrequencyDroopSettingsType**

The elements of this message are used according to Table L.26.

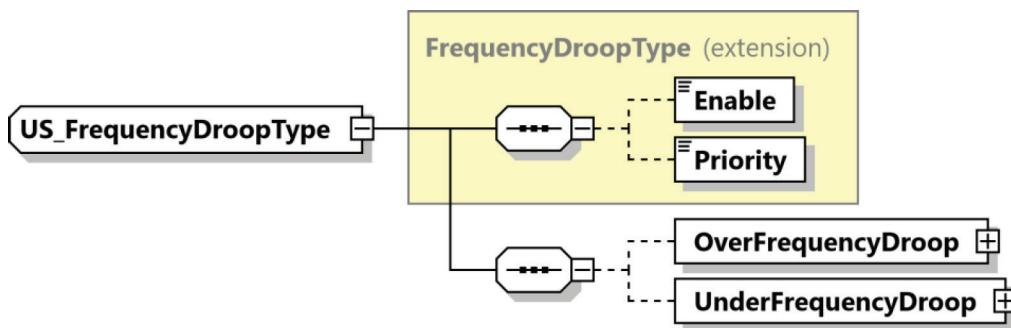
**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table L.26 — Semantics and type definition for EU_FrequencyDroopSettingsType

ElementName	Type	Semantics
Fstart	complexType: RationalNumberType refer to 8.3.5.3.8	Unit: Hz Frequency threshold for activating P(f) control
s	complexType: RationalNumberType refer to 8.3.5.3.8	Unit: Percentage Slope of the P(f) droop
DeactivationTime	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Unit: seconds Time required for the frequency to remain within a stable range, before service deactivation. If the grid frequency returns to a stable band for a period of time equal or higher than the 'DeactivationTime', then the system shall terminate the droop service and return to normal operation in linear mode, with a transient of not less than the 'DeactivationTime' value.
IntentionalDelayPowerControl	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Unit: seconds Delay after which the power shall be adjusted following a frequency change
PowerReference	simpleType: powerReferenceType enumeration refer to L.2.2.2.6	Reference for power adjustment. It can be either the maximum power or the momentary power. If the selected option "MaximumDischargePower" is selected, this refers to the minimum value between EVMaximumDischargePower and EVSENominalPower. If the selected option is "PresentActivePower", this corresponds to the power being discharged at the moment when the frequency reaches Fstart and the Droop is activated.
HysteresisControl	complexType HysteresisControlType refer to L.2.2.1.26	Optional When present provides parameters that describe an "hysterethical" behavior of when frequency goes in the direction of stability.
MaxReactionTime	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Unit: seconds Maximum response time of the system for a new power target setpoint given a new frequency value.

L.2.2.1.24 US_FrequencyDroopType

[V2G20-3183] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.27 and Figure L.27.

- Entwurf -**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)****Figure L.27 — Schema diagram – US_FrequencyDroopType**

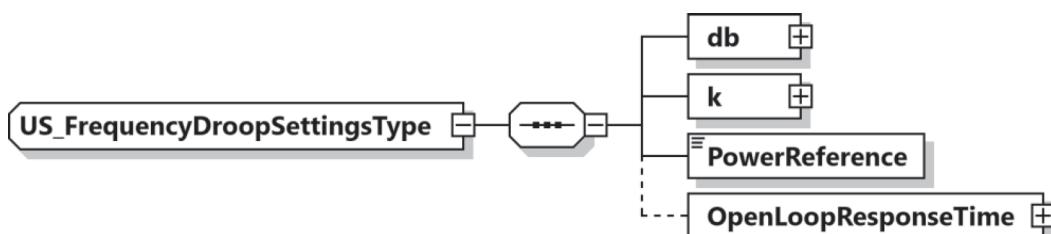
The elements of this message are used according to Table L.27.

Table L.27 — Semantics and type definition for US_FrequencyDroopType

ElementName	Type	Semantics
Enable	simpleType: xs:boolean	Optional Enables the function if set to TRUE. Corresponds to the DHFW.Mod and DLFW.Mod attribute in IEC 61850-7-420:2021.
Priority	simpleType: xs:unsignedShort	Optional Defines the priority of this function in respect to others. Priority = 0 is the highest.
OverFrequencyDroop	complexType: US_FrequencyDroopSettingsType refer to L.2.2.1.25	Optional Values for the Over Frequency Droop curve. If this field is not present, then the UnderFrequencyDroop shall be provided. Corresponds to the DHFW.HzWCrv attribute in IEC 61850-7-420:2021.
UnderFrequencyDroop	complexType: US_FrequencyDroopSettingsType refer to L.2.2.1.25	Optional Values for the Under Frequency Droop curve. If this field is not present, then the OverFrequencyDroop shall be provided. Corresponds to the DLFW.HzWCrv attribute in IEC 61850-7-420:2021.

L.2.2.1.25 US_FrequencyDroopSettingsType

[V2G20-3184] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.28 and Figure L.28.

**Figure L.28 — Schema diagram – US_FrequencyDroopSettingsType**

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

The elements of this message are used according to Table L.28.

Table L.28 — Semantics and type definition for US_FrequencyDroopSettingsType

ElementName	Type	Semantics
db	complexType: RationalNumberType refer to 8.3.5.3.8	Value for the dead band (db) threshold in Hz for which the droop gets activated. In the literature (eg IEEE 2030.5) appears as dbOF or dbUF, for the over and under frequency thresholds respectively.
k	complexType: RationalNumberType refer to 8.3.5.3.8	Droop factor. In the nomenclature is given as kOF and kUF, for the OverFrequency and UnderFrequency curves, respectively. The droop has no unit but it is connected directly to the gradient of the curves. The gradient of a droop curve is $g = \frac{1}{k \times f_n}$, where f_n is the nominal frequency.
PowerReference	simpleType: powerReferenceType enumeration refer to L.2.2.2.6	Reference for power adjustment. It can be either the maximum power or the momentary power. If the selected option “MaximumDischargePower” is selected, this refers to the minimum value between EVMaximumDischargePower and EVSENominalPower. If the selected option is “PresentActivePower”, this corresponds to the power being discharged at the moment when the frequency reaches db and the Droop is activated.
OpenLoopResponseTime	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Unit: Seconds It is the time to ramp up to 90 % of the new target in response to the change in frequency

L.2.2.1.26 HysteresisControlType

[V2G20-3185] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.29 and Figure L.29.

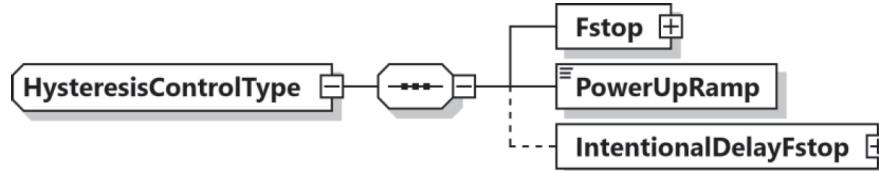


Figure L.29 — Schema diagram – HysteresisControlType

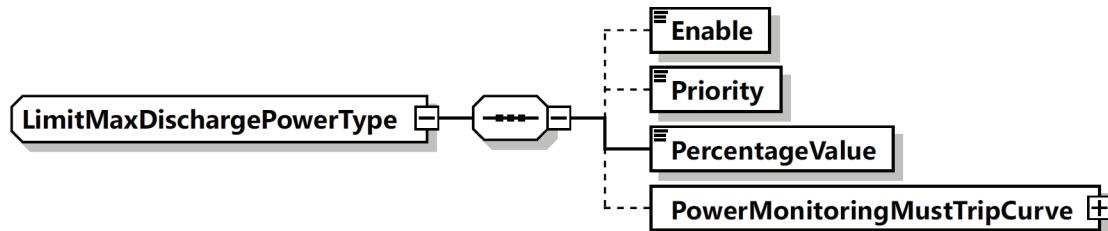
The elements of this message are used according to Table L.29.

Table L.29 — Semantics and type definition for HysteresisControlType

ElementName	Type	Semantics
Fstop	complexType: RationalNumberType refer to 8.3.5.3.8	Frequency that when reached stops the hysteresis behavior and the inverter is allowed again to provide 100 % of the power before the fault.
PowerUpRamp	simpleType: xs:unsignedShort	Unit: Percentage of the Nominal Power per minute.
IntentionalDelayFstop	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Unit: seconds Delay after which the generator is allowed to increase the power according to PowerUpRamp after reaching Fstop.

L.2.2.1.27 LimitMaxDischargePowerType

[V2G20-3186] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.30 and Figure L.30.

**Figure L.30 — Schema diagram - LimitMaxDischargePowerType**

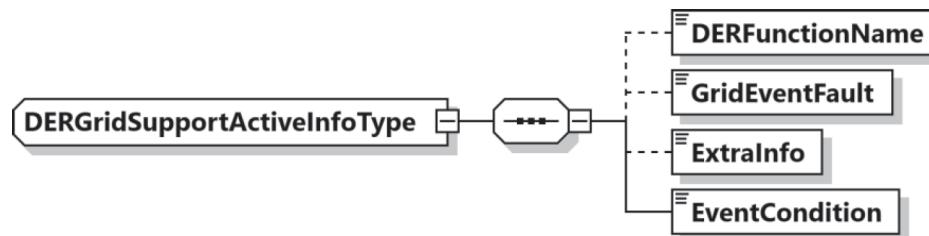
The elements of this message are used according to Table L.30.

Table L.30 — Semantics and type definition for LimitMaxDischargePowerType

ElementName	Type	Semantics
Enable	simpleType: xs:boolean	Optional Enables the function if set to TRUE. Corresponds to the DWMX.Mod attribute in IEC 61850-7-420:2021.
Priority	simpleType: xs:unsignedShort	Optional Defines the priority of this function in respect to others. Priority = 0 is the highest. Corresponds to the DWMX.ModPrio attribute in IEC 61850-7-420:2021.
PercentageValue	simpleType: xs:unsignedShort	Percentage value of the rated EVMaximumDischargePower, reported in the ChargeParameterDiscoveryRequest message. The value lies between 0 and 100. Corresponds to the DWMX.WLimPct attribute in IEC 61850-7-420:2021.
PowerMonitoringMustTripCurve	complexType: DERCurveType refer to L.2.2.1.18	Optional The curve is an interpolation of data points where the abscissa values are time in seconds and the ordinate values refer to the percentage value of the rated EVMaximumDischargePower, reported in the ChargeParameterDiscoveryRequest message. The value lies between 0 and 100. The curve is activated when the power value measured via the ExternalMeter value reported in the ChargeLoopRes is higher than the PercentageValue defined in the previous field. If the power does not stay within the defined curve for the respective period, the EV shall trip.

L.2.2.1.28 DERGridSupportActiveInfoType

[V2G20-3187] [DER] The EVCC and the SECC shall implement the message elements as defined in Table L.31 and Figure L.31.

**Figure L.31 — Schema diagram – DERGridSupportActiveInfoType**

The elements of this message are used according to Table L.31.

Table L.31 — Semantics and type definition for DERGridSupportActiveInfoType

ElementName	Type	Semantics
DERFunctionName	simpleType: DERFunctionNameType Enumeration refer to L.2.2.2.2	Optional Function which was activated due to a grid event and that the EV is performing (eg VoltVar, FreqDroop, ...)
GridEvent	simpleType: GridEventFaultType Enumeration refer to L.2.2.2.3	Optional Event that caused the support to be triggered.
ExtraInfo	simpleType: ExtraInfoType	Optional string[160] Info message with more details about the event and the expected operation of the EV
EventCondition	simpleType: xs:boolean 0: Ended 1: Started	Once a grid event has started and the EV is supporting the grid, a 'Started' condition will be set. Once the support is finished, an 'Ended' condition will be set.

L.2.2.2 AC DER physical values and simple types

[V2G20-3188] [DER] The EVCC and the SECC shall implement the message types as defined in this sub-clause.

L.2.2.2.1 curveDataPointsUnitType**Table L.32 — Name and Description of curveDataPointsUnitType**

Enumeration Name	Description
V	Volts SI unit.
Hz	Hertz SI unit
W	Watts SI unit.
s	Seconds SI unit.
var	Volt-ampere reactive SI unit.
PercentageMaximumConfiguredDischargePower	Percentage of the minimum rated value between EV and EVSE, reported during ChargeParameterDiscovery: min(EVMaximumDischargePower, EVSEMaximumDischargePower).
PercentageMaximumConfiguredDischargeReactivePower	Percentage of the minimum rated value between EV and EVSE, reported during ChargeParameterDiscovery: min(EVMaximumDischargeReactivePower, EVSEMaximumDischargeReactivePower).
PercentageMaximumConfiguredChargePower	Percentage of the minimum rated value between EV and EVSE, reported during ChargeParameterDiscovery: min(EVMaximumChargePower, EVSEMaximumChargePower).

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table L.32 (continued)

Enumeration Name	Description
PercentageMaximumConfiguredChargeReactive-Power	Percentage of the minimum rated value between EV and EVSE, reported during ChargeParameterDiscovery: $\min(\text{EVMaximumChargeReactivePower}, \text{EVSEMaximumChargeReactivePower})$.
PercentageMaximumAvailableDischargePower	Percentage of the the value that results from the difference between the rated EVMaximumDischargePower reported in the CPD and the power value the EV is discharging with, which is reported by the EVPresentActivePower during the CL. If the EV is charging, then EVPresentActivePower will be positive and for the following calculation it shall be considered a value of 0 W for it: $\text{abs}(\text{EVMaximumDischargePower}-\text{EVPresentActivePower})$
PercentageMaximumAvailableDischargeReactive-Power	Percentage of the the value that results from the difference between the rated EVMaximumDischargeReactivePower reported in the CPD and the power value the EV is discharging with, which is reported by the EVPresentReactivePower during the CL. If the EV is charging, then EVPresentReactivePower will be positive and for the following calculation it shall be considered a value of 0 W for it: $\text{abs}(\text{EVMaximumDischargeReactivePower}-\text{EVPresentReactivePower})$

L.2.2.2.2 DERFunctionNameType**Table L.33 — Name and Description of DERFunctionNameType**

Enumeration Name	Description
EnterService	Enter Service function
HFTrip	High Frequency Trip function
LFTrip	Low Frequency Trip function
HVTrip	High Voltage Trip function
LVTrip	Low Voltage Trip function
FrequencyDroop	Frequency Droop function
FrequencyWatt	Frequency-Watt function
VoltWatt	Volt-Watt function
LimitMaxPower	Limit Max Power function
ConstantPFIInjection	Constant-PF Injection function
ConstantPFAbsorption	Constant-PF Absorption function
ConstantVarInjection	Constant-Var Injection function
ConstantVarAbsorption	Constant-Var Absorption function
VoltVar	Volt-Var function
WattVar	Watt-Var function
WattCosPhi	Watt-CosPhi function

L.2.2.2.3 gridEventFaultType**Table L.34 — Name and Description of gridEventFaultType**

Enumeration Name	Description
OverCurrent	Over current detected
OverVoltage	Over voltage detected
UnderVoltage	Under voltage detected
OverFrequency	Over frequency detected
UnderFrequency	Under frequency detected
VoltageImbalance	Voltage imbalance detected
CurrentImbalance	Current imbalance detected
EmergencyLocal	Local emergency detected
LowPowerInput	Low power input detected
PhaseRotation	Phase rotation detected

L.2.2.2.4 powerDuringCessationType**Table L.35 — Name and Description of powerDuringCessationType**

Enumeration Name	Description
ActivePower	Feed-in during cessation with Active Power
ReactivePower	Feed-in during cessation with Reactive Power

L.2.2.2.5 powerFactorExcitationType**Table L.36 — Name and Description of powerFactorExcitationType**

Enumeration Name	Description
Over-Excited	Power Factor value for injected reactive power
Under-Excited	Power Factor value for absorbed reactive power

L.2.2.2.6 powerReferenceType**Table L.37 — Name and Description of powerReferenceType**

Enumeration Name	Description
MaximumDischargePower	The reference used is the minimum between the EVSEMaximumDischargePower and EVSENominalPower
PresentActivePower	The reference used is the present active power at the moment of the droop activation

L.2.2.2.7 lockValueUnitType**Table L.38 — Name and Description of lockValueUnitType**

Enumeration Name	Description
V	Volts SI unit.
Hz	Hertz SI unit
W	Watts SI unit.
s	Seconds SI unit.
var	Volt-ampere reactive SI unit.

L.3 Service selection

If the AC DER service is selected, the requirements in 8.4.1 and 8.4.2 apply.

L.3.1 Selection of service and service parameters

If the AC DER service is selected, the requirements in 8.4.3.1 apply.

L.3.1.1 Service parameters for the AC DER service

L.3.1.1.1 General

If the AC DER service is selected, the requirement in 8.4.3.2.1 applies.

L.3.1.1.2 AC DER service and bitmap

[V2G20-3189] [DER] The EVCC and the SECC shall implement the ServiceParameterList for the AC DER service as defined Table L.39.

Table L.39 — Configuration parameters for AC_DER

ParameterName	ParameterType	Values	Description
Connector	intValue	1: SinglePhase 2: ThreePhase	Usage of the connector.
ControlMode	intValue	1: Scheduled 2: Dynamic	Selection of which party (SECC or EVCC) is responsible to fulfill the mobility needs of this service session.
MobilityNeedsMode	intValue	1: Mobility needs provided by EVCC 2: Mobility needs provided by SECC allowed	Indicate who can provide mobility needs information. Value 2 indicates that not only EVCC but also SECC can provide mobility-needs information (however, the EVCC shall always provide an initial mobility-needs information including DepartureTime). Value 2 can be selected only if Dynamic ControlMode was selected.
BPTChannel	intValue	1: Unified 2: Separated	Type of installed power transfer channel. Unified: Single channel Separated: Dual channel
DERStandardControlFunctions	intValue	refer to L.3.1.1.2.1	Bitmap used by the SECC to inform the EVCC about the minimum DER standard functions it expects the EV to support. Refer to table DERStandardControlFunctions Bitmap for the decoding of the bitmap. This bitmap is a 1:1 mapping of the IEEE 2030.5 DERControlType object.
DERExtendedControlFunctions	intValue	refer to L.3.1.1.2.2	Bitmap used by the SECC to inform the EVCC the minimum DER extended functions it expects the EV to support. Refer to table DER-ExtendedControlFunctions Bitmap for the decoding of the bitmap.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

- [V2G20-3190] [DER]** The SECC shall provide the DER functions it demands the EVCC to support using the DERStandardControlFunctions parameter and the DERExtendedControlFunctions parameter.
- [V2G20-3191] [DER]** The EVCC shall only select the AC DER service, if it supports all control functions that were enabled (i.e., the corresponding bits were set to '1').
- [V2G20-3192] [DER]** The SECC and the EVCC shall not send any parameters that are not relevant to one of the control functions that were enabled in either the DERStandardControlFunctions or DERExtendedControlFunctions parameter.
- [V2G20-3193] [DER]** In case the AC DER service was selected, unless otherwise stated, anytime an element is prefixed with DER or AC (e.g. DER_AC_CPDReqEnergyTransferMode), it shall be used. In case both elements are available exclusively, DER takes precedence.

L.3.1.1.2.1 DERStandardControlFunctionsBitmap

- [V2G20-3194] [DER]** The EVCC and the SECC shall implement the DERStandardControlFunctionsBitmap for the AC DER service as defined in Table L.40.
- [V2G20-3195] [DER]** For all control functions that the EVCC and the SECC implement, all related parameters mentioned in the "ISO 15118 DER Function" column of Table L.40 shall be implemented.

Table L.40 — Configuration parameters for AC_DER

Bit	Description	ISO 15118 DER Function
0 (LSB)	Charge mode support	Inherent to ACBPT - This is bit is always set to 1
1	Discharge mode support	Inherent to ACBPT - This is bit is always set to 1
2	Ability to disconnect and reconnect to the grid via galvanic isolation	No equivalent function in ISO 15118-20
3	The ability to remotely authorize/deauthorize the EV to discharge at the site	Associated with EnterServiceType: PermitService
4	Fixed power factor setpoint when absorbing active power (Under-excited)	Associated with ReactivePowerSupportType: ConstantPowerFactor (PowerFactorExcitation == Under-Excited)
5	Fixed power factor setpoint when injecting active power (Over-excited)	Associated with ReactivePowerSupportType: ConstantPowerFactor (PowerFactorExcitation == Over-Excited)
6	Reactive power setpoint	Associated with ReactivePowerSupportType: ConstantVar
7	not used by this document	
8	Frequency-Watt Parameterized mode (Droop Curve)	Associated with ActivePowerSupportType: US_FrequencyDroopSettingsType
9	Frequency-Watt Curve mode	Associated with ActivePowerSupportType: FrequencyWatt
10	High Frequency Ride-Through, May Trip mode	Associated with EnterServiceType: FrequencyTrip (OverFrequencyMayTripCurve)
11	High Frequency Ride-Through, Must Trip mode	Associated with EnterServiceType: FrequencyTrip (OverFrequencyMustTripCurve)
12	High Voltage Ride-Through, May Trip mode	Associated with EnterServiceType: VoltageTrip (OverVoltageMayTripCurve)
13	High Voltage Ride-Through, Momentary Cessation mode	Associated with EnterServiceType: VoltageTrip (OverVoltageMomentaryCessationTripCurve)

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

Table L.40 (continued)

Bit	Description	ISO 15118 DER Function
14	High Voltage Ride-Through, Must Trip mode	Associated with EnterServiceType: VoltageTrip (OverVoltageMustTripCurve)
15	Low Frequency Ride-Through, May Trip mode	Associated with EnterServiceType: FrequencyTrip (UnderFrequencyMayTripCurve)
16	Low Frequency Ride-Through, Must Trip mode	Associated with EnterServiceType: FrequencyTrip (UnderFrequencyMustTripCurve)
17	Low Voltage Ride-Through, May Trip mode	Associated with EnterServiceType: VoltageTrip (UnderVoltageMayTripCurve)
18	Low Voltage Ride-Through, Momentary Cessation mode	Associated with EnterServiceType: VoltageTrip (UnderVoltageMomentaryTripCurve)
19	Low Voltage Ride-Through, Must Trip mode	Associated with EnterServiceType: VoltageTrip (UnderVoltageMustTripCurve)
20	Limitation of the maximum active power	Associated with ActivePowerSupportType: LimitMaxDischargePower
21	Target reactive power in absolute value	Associated with ChargeLoopRes field: EVSETTargetReactivePower
22	Target active power in absolute value	Associated with ChargeLoopRes field: EVSETTargetActivePower
23	Volt-Var mode	Associated with ReactivePowerSupportType: VoltVar
24	Volt-Watt mode	Associated with ActivePowerSupportType: VoltWatt
25	Watt-Power factor/WattCosPhi mode	Associated with ReactivePowerSupportType: WattCosPhi
26	Watt-Var mode	Associated with ReactivePowerSupportType: WattVar

- [V2G20-3196] [DER]** If the control function identified by bit '3' is enabled and if PermitService = FALSE in the EnterServiceType parameters, the EV shall cease to energize. While PermitService = FALSE, any request by the SECC to discharge shall be ignored by the EVCC and can only take effect after the EV is back in service.
- [V2G20-3197] [DER]** If the control function identified by bit '3' is enabled and if PermitService = FALSE in the EnterServiceType parameters and if the EV is trying to discharge, the SECC shall stop the communication.
- [V2G20-3198] [DER]** If the optional Enable parameter is not present, it shall be treated as if Enable = TRUE.
- [V2G20-3199] [DER]** If more than one Enable parameter of a control function is set to TRUE, the EVCC shall use the Priority parameter to determine which control function takes precedence.
- [V2G20-3200] [DER]** If Scheduled control mode is used in conjunction with the AC DER service, any control function shall take precedence over the currently applicable schedule.

**E DIN EN ISO 15118-20/A1:2025-02
ISO 15118-20:2022/DAM 1:2024(en)**

L.3.1.1.2.2 DERExtendedControlFunctionsBitmap

[V2G20-3201] [DER] The EVCC and the SECC shall implement the DERExtendedControlFunctionsBitmap for the AC DER service as defined in Table L.41.

[V2G20-3202] [DER] For all control functions that the EVCC and the SECC implement, all related parameters mentioned in the "ISO 15118 DER Function" column of Table L.41 shall be implemented.

Table L.41 — Configuration parameters for AC_DER

Bit	Description	ISO 15118 DER Function
0 (LSB)	Frequency-Watt Curve mode according to AS/NZS 4777.2 Clause 4.5.3	Associated with ActivePowerSupportType function fields: FrequencyWatt HysteresisHigh HysteresisLow HysteresisDelay HysteresisGradient
1	FrequencyDroop according to EN 50549	Associated with ActivePowerSupportType function fields: EU_FrequencyDroopSettingsType
2	DCInjectionRestriction	Associated with DER Control type: MaximumLevel1DCInjection MaximumLevel2DCInjection
3	Zero Current Mode	When a OVRT or UVRT occurs, the power converter shall stop the power electronics from switching (pulse lock). Associated with FaultRideThroughType field: DeadBand
4	Over Voltage Fault Ride Through (OVRT)	Associated with FaultRideThroughType fields: OverVoltageRideThroughPositive OverVoltageRideThroughNegative
5	Under Voltage Fault Ride Through (UVRT)	Associated with FaultRideThroughType fields: UnderVoltageRideThroughPositive UnderVoltageRideThroughNegative
6	Short Circuit Ratio (SCR)	Associated with DERControlType: SCRatPOC

Bibliography

Add the following reference at the end of the Bibliography:

[106] IEEE 802.3-2022, IEEE Standard for Ethernet (July 2022)