International Standard

ISO 15118-20

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

Véhicules routiers — Interface de communication entre véhicule et réseau électrique —

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

AMENDEMENT 1: Service RED en CA, service MCS et concept de sécurité amélioré

First edition
2022-04

AMENDMENT 1
2026-07

Reference number
ISO 15118-20:2022/Amd.1:2026(en)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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 jointly by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 31, *Data communication*, Technical Committee IEC/TC 69, *Electrical power/energy transfer systems for electrically propelled road vehicles and industrial trucks*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 301, *Road vehicles*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

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, Normative references

Add the following references at the end of the clause:

ISO 15118-10:2025, *Road vehicles — Vehicle to grid communication interface — Part 10: Physical layer and data link layer requirements for single-pair Ethernet*

IEC 61851-23-3:2025, *Electric vehicle conductive charging system - Part 23-3: DC electric vehicle supply equipment for Megawatt charging systems*

Clause 3, Terms and definitions

Add the following terms and definitions at the end of the 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
area EPS
area electric power system as defined in IEEE 1547

3.75
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.

3.76
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.

3.77
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 *distributed energy resource (DER)* (3.76) will not be allowed to start injecting power to the grid/electric power system.

3.78
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.

3.79
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 United States of America.

3.80
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 United States of America the voltage supplied is typically 240 Vrms AC whereas in Europe is 230 Vrms AC.

3.81
may trip region
region of voltage or frequency within which the EV is allowed to *cease to energize* (3.75) and to *trip* (3.88) the connection

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

3.82
momentary cessation region
region of voltage or frequency within which the EV will temporarily *cease to energize* (3.75) (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.

3.83
must trip region
region of voltage or frequency within which the EV must *cease to energize* (3.75) and must *trip* (3.88) the connection

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

3.84
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

3.85
permit service
setting that indicates whether a *distributed energy resource (DER)* (3.76) is allowed to enter or remain in service

3.86
return to service
enter service (3.77) following recovery from a *trip* (3.88)

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* (3.86)

Note 1 to entry: Once the *distributed energy resource (DER)* (3.76) has permission to come back to service, it shall follow the *enter service* (3.77) rules.

Clause 4, Abbreviated terms

Add the following abbreviations to the list:

CE charge enable

CL charge loop

DER distributed energy resource (in the context of AC DER)

MCS megawatt charging system

Modify the existing abbreviation DER as follows:

DER distinguished encoding rules (in the context of X.509v3 certificates)

5.2

Replace the entire subclause including its title with the following subclause:

5.2 Requirement and provision structure

This document uses the requirement structure defined here. Also, important provisions that are no requirements (“shall”), but permissions (“may”) or recommendations (“should”) use the structure defined here. A unique number identifies each individual requirement or provision defined in this document. Systematic and ordered requirement (provision) structure enables readers to find the target requirement (provision) number easily.

The following format is applied for newly added and updated requirements or provisions:

"[V2G20-"XXXX"]" "requirement/provision text", where:

— "V2G20" represents this document;

— “XXXX” represents the unique requirement or provision number consisting of four digits starting from 1 000;

— "requirement/provision text" includes the actual text of the requirement or provision.

— For purely AC DER or MCS specific requirements, an identifier is added as follows: "[V2G20-"XXXX"] [DER]" or "[V2G20-"XXXX"] [MCS]”, respectively.

EXAMPLE 1 **[V2G20-0000]** This shall/may/should be an example requirement introduced in this document.

The following format is applied for requirements taken over from ISO 15118-2 Ed.1:

[“V2G20”-"YYY"] "requirement/provision text", where:

— "V2G20" represents this document;

— “YYY” represents the unique requirement or provision number as already defined in ISO 15118-2 Ed.1;

— "requirement/provision text" is the same text as specified in ISO 15118-2 Ed.1.

EXAMPLE 2 **[V2G20-000]** This shall/may/should be an example requirement originally defined in ISO 15118-2 Ed.1.

Clause 6

Replace Figure 2 with this figure:

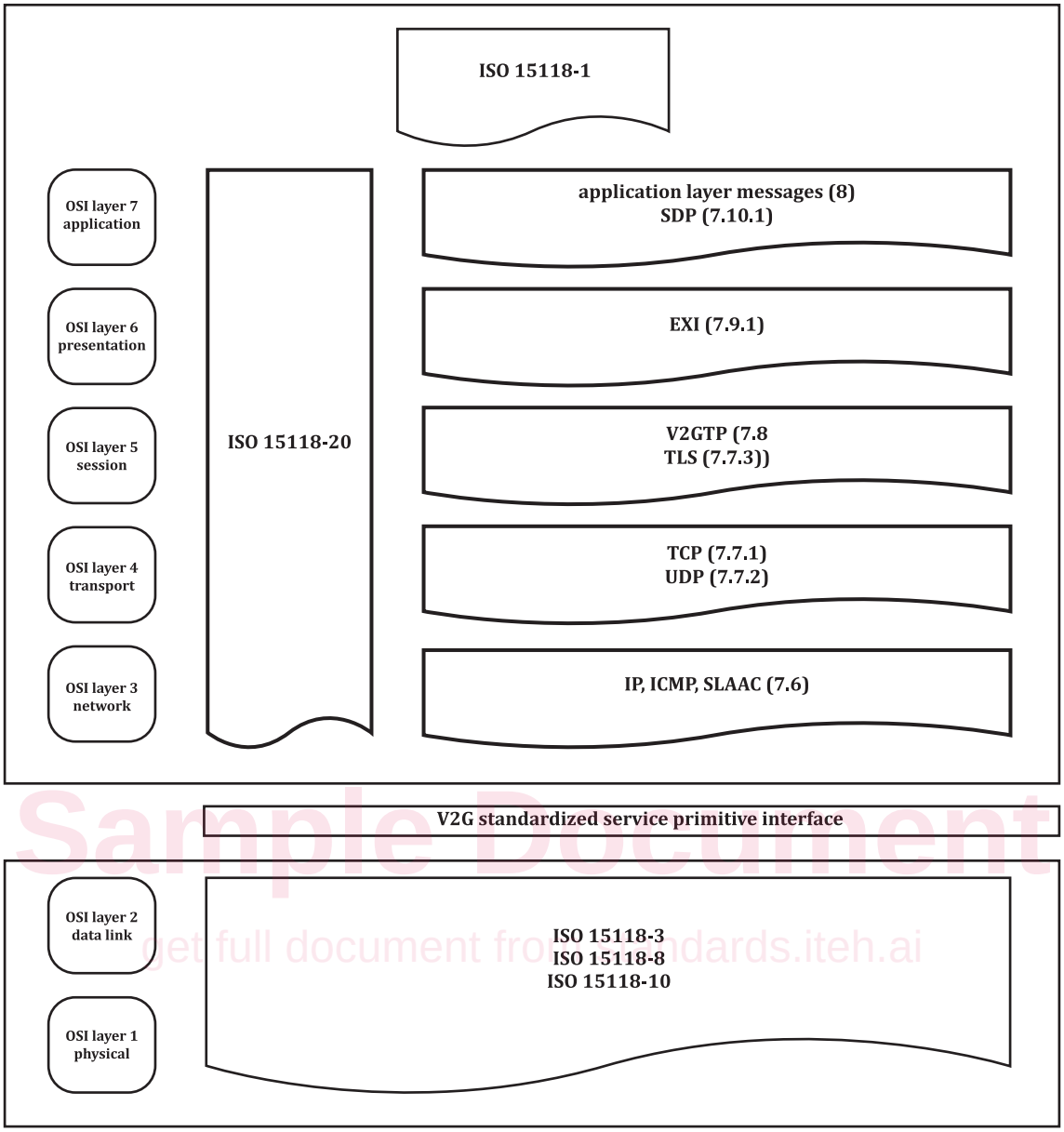


Figure 2 — Vehicle to grid communication document overview

7.3.2

Replace Table 2 with this table:

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	Further specification of key usage using OIDs, e.g.: — server authentication (1.3.6.1.5.5.7.3.1) — client authentication (1.3.6.1.5.5.7.3.2) NOTE Sometimes the following values are encoded here: — Netscape SGC (1.3.6.1.4.1.311.10.3.3) — Microsoft SGC (2.16.840.1.113730.4.1) 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.
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

Replace NOTE 8 with:

NOTE 8 Additionally, key length of 456 bits is used with certain curves in the application of this document. If a V2G entity can manage and utilize 521 bit keys, it can be capable of managing and utilizing 456 bit keys as well.

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 1 600 bytes. This limit considers resource constraints in embedded systems. To reduce the size of certificates, things to consider are for example to be cautious when adding long URLs, 4-byte characters in distinguished names, or multiple certificate policies as these can 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 1 600 bytes.

Replace the 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 [...].

a) 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.

7.3.2.1

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

[V2G20-3002] The OCSP signer certificate used to sign the OCSP response for the 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 "certificate_authorities" 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 the requirements [V2G20-2330] and [V2G20-2332] with the following new requirements, respectively:

[V2G20-3003] The OCSP signer certificate used to sign the OCSP response for the contract certificate status shall be generated using a certificate chain that uses either the same eMSP root CA certificate or the same V2G root CA certificate as the trust anchor of 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] The OCSP signer certificate used to sign the OCSP response for the 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 of 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 the requirement [V2G20-2334] and NOTE 12 with:

[V2G20-3005] The OCSP signer certificate used to sign the OCSP response for the 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.

7.3.4

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

7.4

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

[V2G20-3006] [MCS] In case of an 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 15118-10:2025, 7.6.

[V2G20-3007] [MCS] In case of an 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 15118-10:2025, 7.6.

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

7.5

Replace second sentence of the first paragraph with:

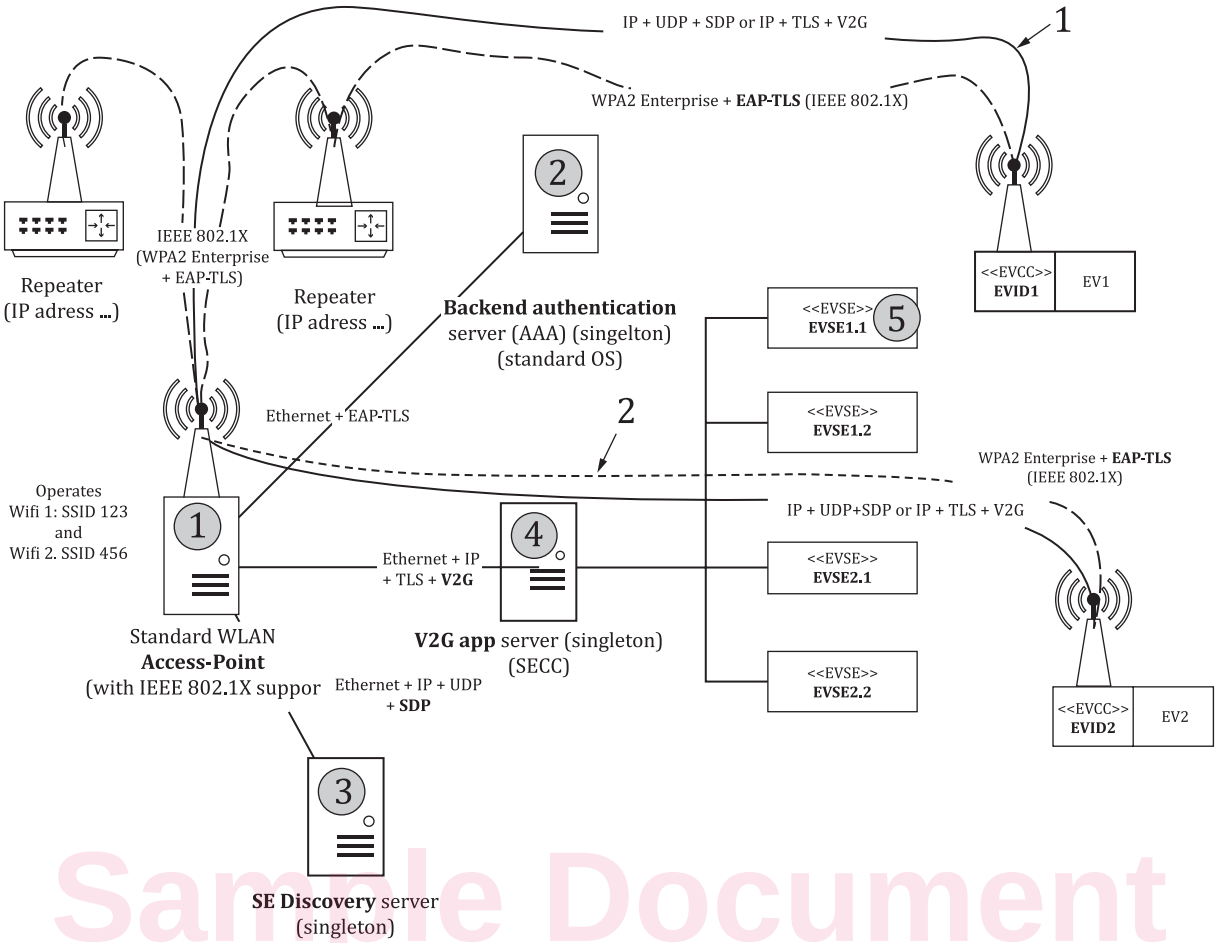
ISO 15118-3, ISO 15118-8, and ISO 15118-10 define additional details on data link layer to be covered.

Add the following new requirement at the end of this subclause:

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

7.5.1.2

Replace Figure 10 with this figure:



Key

1 App layer communication protocol

2 IEEE 802.1X communication protocol

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

7.7.3.3

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 5280:2008, 4.1.2.4 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399) for root certificates these RDNs must be the same between the Issuer field and the subject field.

Replace the requirements [V2G20-2369], [V2G20-2370] with the following new requirements, respectively:

[V2G20-3373] If no V2G root CA certificate(s) and PE private root CA certificate(s) are available in the EVCC, "certificate_authorities" extension shall not be present in the "ClientHello" message.

[V2G20-3374] While the EVCC is in CPM4PE, it shall not include "certificate_authorities" extension in the "ClientHello" message regardless if the EVCC has any V2G root CA certificate(s) and PE private root CA certificate(s) or not. Refer to H.2.2.3 for details of CPM4PE.

Delete the following requirement: [V2G20-2371]

Replace the requirements [V2G20-2378], [V2G20-2379] with the following new requirements, respectively:

[V2G20-3375] If the EVCC did not provide any indication of the available roots according to **[V2G20-3373]**, a public SECC shall send in the "ServerHello" message its own certificate chain (SECC certificate chain) including any necessary cross certificates up to a root (excluding the root certificate itself) of its own choosing.

[V2G20-3376] If the EVCC provides a list of the available roots according to [V2G20-1006], the public SECC shall follow IETF RFC 5280:2008, 7.1, as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399, to utilize the received "DistinguishedNames" (see [V2G20-1006]) to choose an SECC certificate chain originating from one of the received "DistinguishedNames" and provide it to the EVCC in "ServerHello" message as defined in IETF RFC 8446.

Replace the requirements [V2G20-2383], [V2G20-2384] with the following new requirements, respectively:

[V2G20-3377] If the EVCC provides a list of the available roots according to [V2G20-1006], the private SECC shall follow IETF RFC 5280:2008, 7.1 as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399, to utilize the received "DistinguishedNames" (see [V2G20-1006]) to choose a PE certificate chain originating from one of the received "DistinguishedNames" and provide it to the EVCC in "ServerHello" message as defined in IETF RFC 8446.

[V2G20-3378] If the EVCC did not provide any indication of the available roots according to **[V2G20-3373]**, a private SECC not in CPM4PE shall send in the "ServerHello" message its own certificate chain (PE certificate chain) including any necessary cross-certificates up to a root (excluding the root certificate itself) of its own choosing.

Replace the requirement [V2G20-2388] with:

[V2G20-3379] Since the EVCC used the "status_request" extension to request OCSP response for the certificate chain sent by the public SECC, it shall include an OCSP response for each certificate in the certificate chain sent by the public SECC in the "Certificate" message. Refer to IETF RFC 6960 (as updated by IETF RFC 8954) and IETF RFC 8446 for further details.

Replace the requirement [V2G20-2391] with:

[V2G20-3380] Since the EVCC used the "status_request" extension to request OCSP response for the certificate chain sent by private SECC, if the private SECC supports PnC, it shall include an OCSP response for each certificate in the certificate chain sent by the private SECC in the "Certificate" message. Refer to IETF RFC 6960 (as updated by IETF RFC 8954) and IETF RFC 8446 for further adetails.

Replace NOTE 21 below [V2G20-1008] with:

NOTE 21 As defined in IETF RFC 6960 (as updated by IETF RFC 8954), an OCSP responder can either be the sub-CA itself, or it can 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.

Replace the requirements [V2G20-2404], [V2G20-2405] with the following new requirements, respectively:

[V2G20-3381] If no V2G root CA certificate and OEM root CA certificate is/are available in the public SECC or private SECC not in CPM4PE, the "certificate_authorities" extension shall not be present in the "CertificateRequest" message.

[V2G20-3382] A private SECC in CPM4PE shall send not include "certificate_authorities" extension in the "CertificateRequest" message. Refer to H.2.2.3 for details of CPM4PE.

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 5280:2008, 4.1.2.4 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399) for root certificates these RDNs must be the same between the Issuer field and the Subject field.

Replace the requirements [V2G20-2426], [V2G20-2427], [V2G20-2428] with the following new requirements, respectively:

[V2G20-3383] If the SECC provides a list of the available roots according to [V2G20-2401] or [V2G20-2402], the EVCC shall follow IETF RFC 5280:2008, 7.1, as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399, to utilize the received "DistinguishedNames" (see [V2G20-2401]) to choose a vehicle certificate chain originating from one of the received "DistinguishedNames" and provide it to the SECC in "Certificate" message as defined in IETF RFC 8446.

[V2G20-3384] If the public SECC did not provide any indication of the available roots according to **[V2G20-3381]**, the EVCC shall send a "Certificate" message containing its own certificate chain (vehicle certificate chain) including any necessary cross-certificates up to the corresponding root (excluding the root certificate itself) of its own choosing.

[V2G20-3385] If the private SECC did not provide any indication of the available roots according to **[V2G20-3381]**, an EVCC not in CPM4PE shall send a "Certificate" message containing its own certificate chain (vehicle certificate chain) including any necessary cross-certificates up to the corresponding root (excluding the root certificate itself) of its own choosing.

Renumber all NOTEs starting from the original NOTE 9.

7.7.3.10

Add the following new requirements and note at the end of the subclause:

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

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

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

7.8.3.1, Table 14

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