



DPC: 24/30481263 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 13 December 2024

Origin: European

Latest date for receipt of comments: 05 February 2025

Project No. 2023/02352

Responsible committee: PEL/69 Electric vehicles

Interested committees:

Title: Draft BS EN ISO 15118-20 :2022/Amd 1 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.

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 05 February 2025

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Responsible Committee Secretary: Ms Andreea Vieru (BSI)

Direct tel: 0208 996 7432

E-mail: andreea.vieru@bsigroup.com

Full document details: 24/30481263 DC

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT Amendment

ISO 15118-20:2022/ DAM 1

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

ICS: 43.120

ISO/TC 22/SC 31

Secretariat: **DIN**

Voting begins on:
2024-12-13

Voting terminates on:
2025-03-07

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

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

© ISO 2024



Documents

Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 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.

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

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:

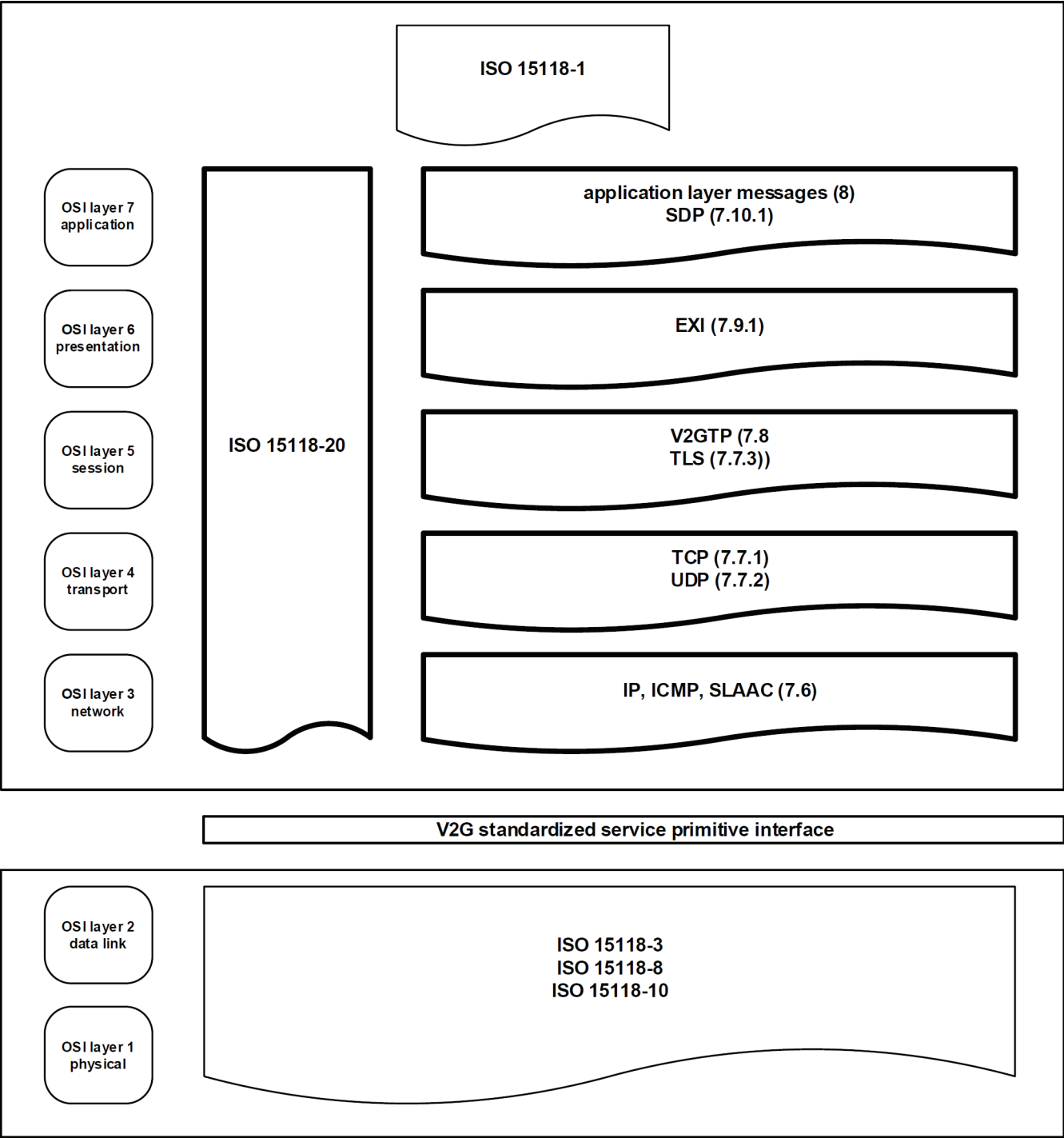


Figure 2 — Vehicle to grid communication document overview

Clause 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

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

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

- [V2G20-3002]** OCSF signer certificate used to sign the OCSF 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 “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 OCSF signer certificate that signs the OCSF 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]** OCSF signer certificate used to sign the OCSF response for 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 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]** OCSF signer certificate used to sign the OCSF 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 OCSF signer certificate that signs the OCSF 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]** OCSF signer certificate used to sign the OCSF 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 OCSF signer certificate that signs the OCSF 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].

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:

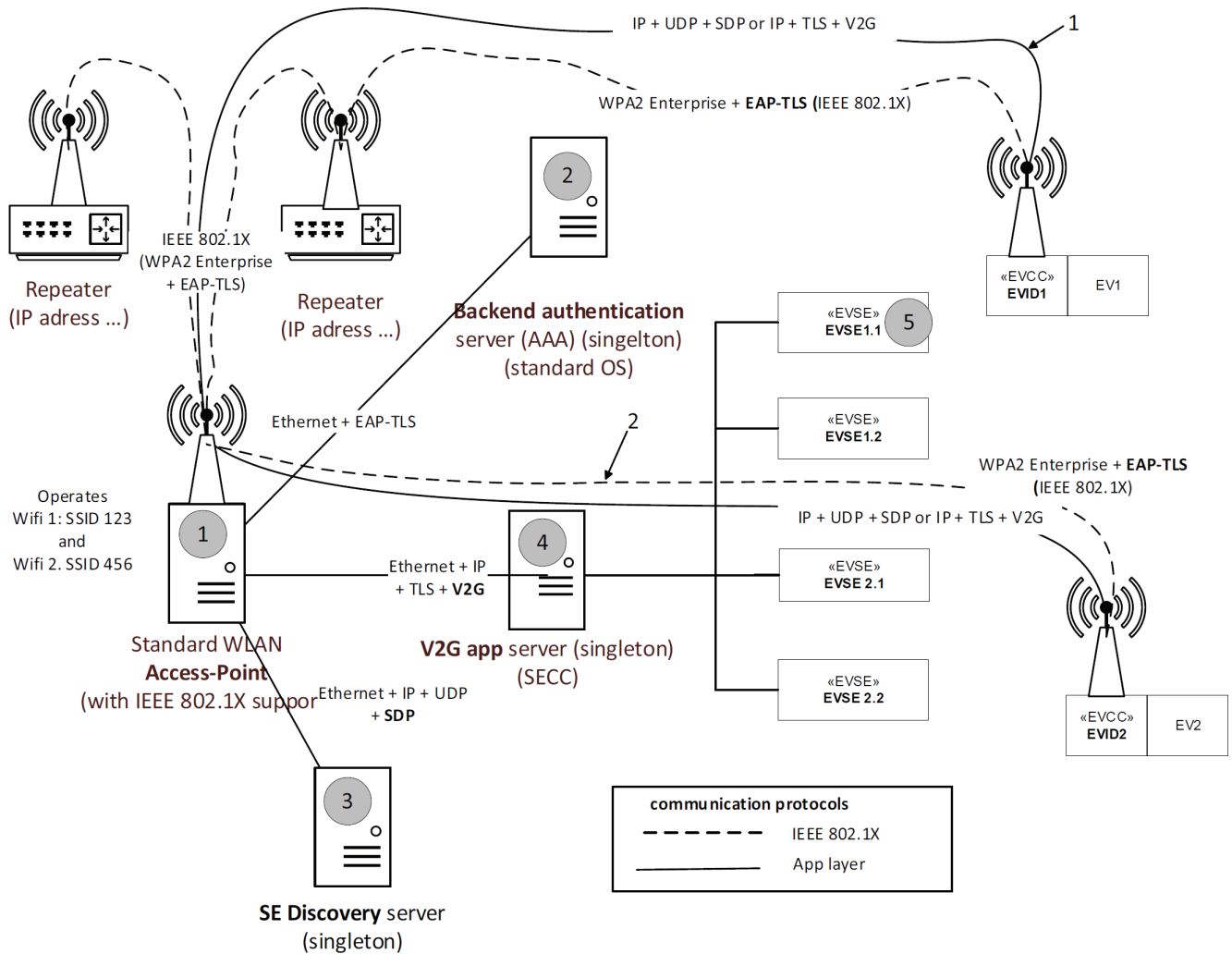
ISO 15118-3, ISO 15118-8, and ISO 15118-10 define additional details on data link layer to be covered.

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:



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.

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 Part20ACDERMainstreamPayloadID 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.

[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:

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:

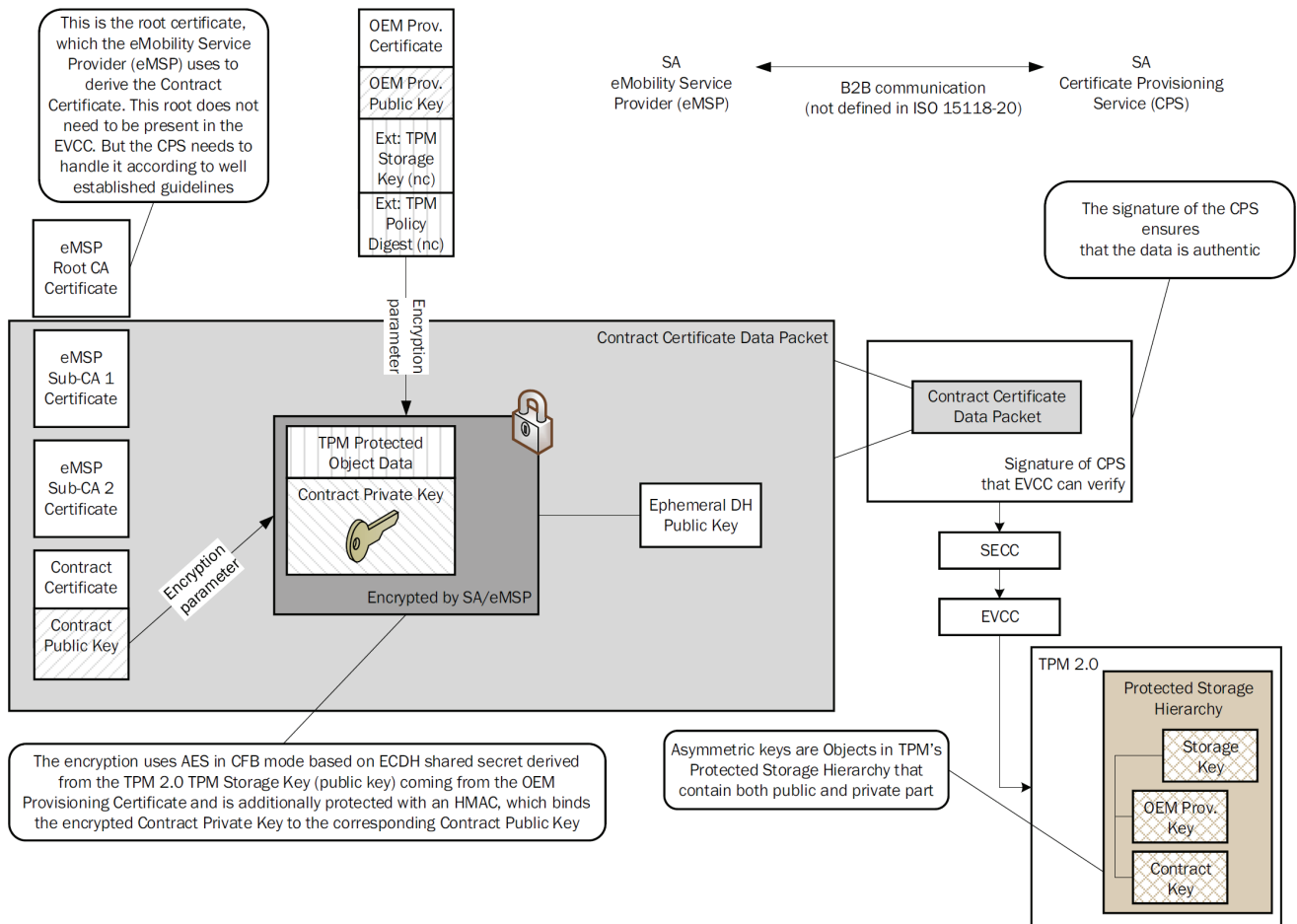


Figure 25 — Process for CertificateInstallationRes for EVCC equipped with TPM 2.0

Clause 7.9.2.5.3.3, Figure 26

Replace Figure 26 with this figure:

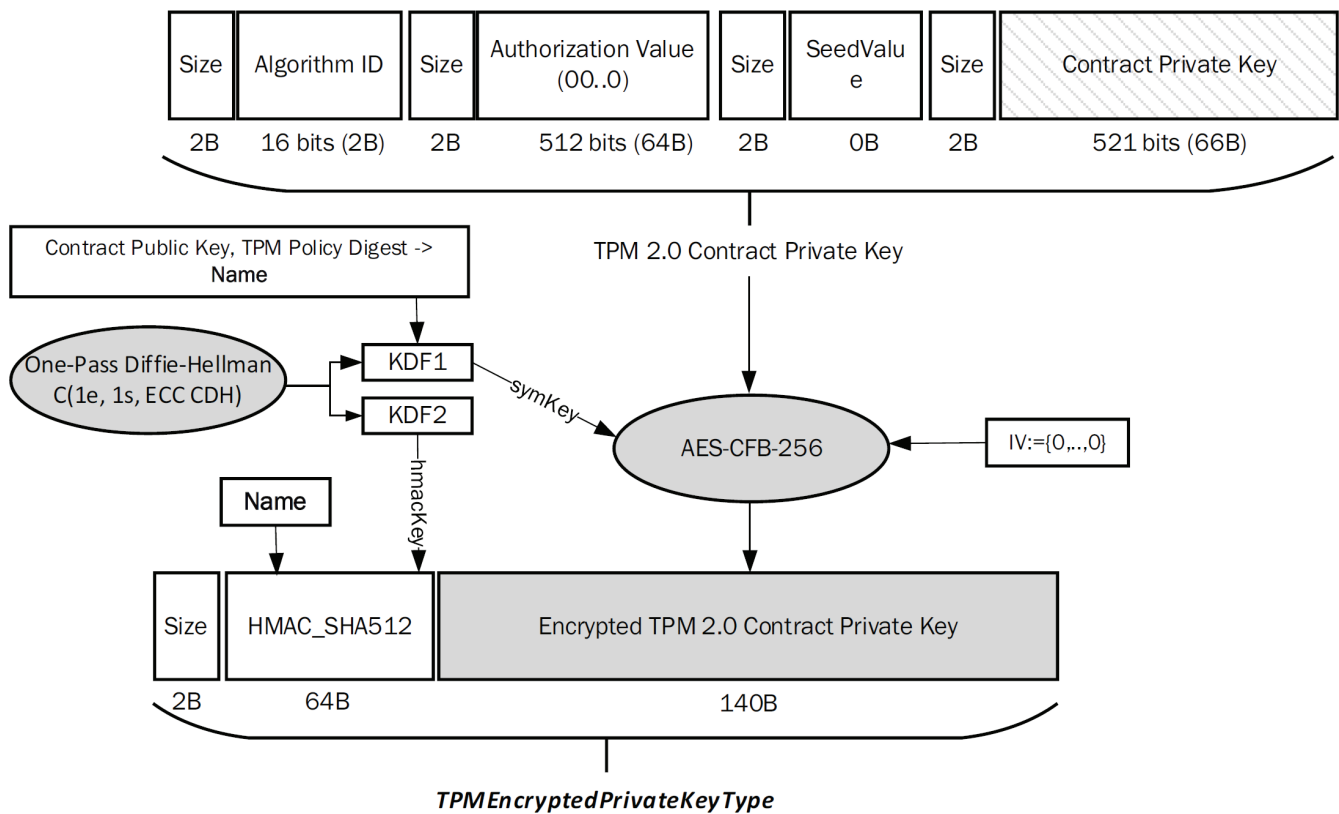


Figure 26 — Contract key encryption for direct import into EVCC's TPM 2.0 (for (elliptic curve) EC P-521/secp521r1)

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):

- [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 SDPRequest-PayloadID (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 SDP-ResponsePayloadID (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

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

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.

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.

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) }

- { 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.

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).

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).

TheOIDrepository^[99]alsoreferstoid-contractDynamicInformationUrlscontractDynamicInformationUrl(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-calIssuers as calIssuers(2) (see NOTE 1 above providing the OID value for id-ad-calIssuers).

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.

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

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).

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.

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

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
		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

Table B.3 (continued)

ISO 15118-20 certificate profiles			V2G Root V2G
TbsCertificate	Subject	Organization Unit (OU)	(x)
		Common Name (CN)	x
		Domain Component (DC)	(x)
	SubjectPublicKeyInfo	AlgorithmIdentifier	x
		algorithm	x id-ecPublicKey
		parameters (ECPParameters)	x
		namedCurve	x secp521r1
		SubjectPublicKey	x (BIT STRING)
	IssuerUniqueID		-
	SubjectUniqueID		-
	Extensions	AuthorityKeyIdentifier	-
		SubjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifier
		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	-

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	x
		algorithm	x id-Ed448
		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)]
	Subject	Country (C)	(x) (ISO 3166-1 alpha-2 code)
		Organization (O)	x
		Organization Unit (OU)	(x)
		Common Name (CN)	x
		Domain Component (DC)	(x)
	SubjectPublicKeyInfo	AlgorithmIdentifier	x
		algorithm	x id-Ed448
		parameters	-
		SubjectPublicKey	x (BIT STRING)

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:

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
		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 CSO]	x [up to CSO]
	Subject	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 SECCID (see [V2G20-2583])
		Domain Component (DC)	(x)	(x) & "CSO"
	Subject-PublicKey-Info	AlgorithmIdentifier	x	x
		algorithm	x id-ecPublicKey	x id-ecPublicKey
		parameters (ECPParameters)	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	x / nc id-ce-authorityKey-Identifier

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	Extensions	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	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
		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)

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-basicCon- straints	x / c id-ce-basicCon- straints
		cA	TRUE	TRUE	FALSE
		pathLenConstraint	1	0	-
		CRLDistribution- Points (CRL)	-	-	-
		AuthorityInfoAc- cess	x / nc id-pe-authorityInfoAc- cess	x / nc id-pe-authorityIn- foAccess	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 responder)	x (URI of the OCSP responder)
		generalName	x uniformResourceI- dentifier [6]	x uniformResourceI- dentifier [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	-
		accessMethod	x id-crossCertIndication (see [V2G20-2604])	x id-crossCertIndica- tion (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 alphanu- meric string with a maximum length of 5 bytes as described here)	x "CROSS" (Syntax: An alphanu- meric string with a maximum length of 5 bytes as described here)	-
		accessDescription	-	-	-

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
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
	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 CSO]	x [up to CSO]	x [up to CSO]

Table B.6 (continued)

ISO 15118-20 certificate profiles			Charge point operator		
			CSO Sub-CA 1 Sub	CSO Sub-CA 2 Sub	SECC Cert Leaf
TbsCertificate	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		-	-	-
		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

Table B.6 (continued)

ISO 15118-20 certificate profiles			Charge point operator		
			CSO Sub-CA 1 Sub	CSO Sub-CA 2 Sub	SECC Cert Leaf
	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-basicCon- straints	x / c id-ce-basicCon- straints
		cA	TRUE	TRUE	FALSE
		pathLenConstraint	1	0	-
		CRLDistribution- Points (CRL)	-	-	-
		AuthorityInfoAc- cess	x / nc id-pe-authorityIn- foAccess	x / nc id-pe-authorityIn- foAccess	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 responder)	x (URI of the OCSP responder)	x (URI of the OCSP responder)
		generalName	x uniformResourceI- dentifier [6]	x uniformResourceI- dentifier [6]	x uniformResourceI- dentifier [6]
		accessDescription	-	-	-

Table B.6 (continued)

ISO 15118-20 certificate profiles			Charge point operator		
			CSO Sub-CA 1 Sub	CSO Sub-CA 2 Sub	SECC Cert Leaf
		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 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]:

- [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
		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 CPS]	x [up to CPS]

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 (ECPParameters)	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	-	-	-
		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

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
TbsCertificate	Extensions	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
		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

Table B.7 (continued)

ISO 15118-20 certificate profiles			Certificate provisioning service		
			CPS Sub-CA 1	CPS Sub-CA 2	CPS Leaf Cert
			Sub	Sub	Leaf
		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 uniformResourceI- dentifier [6]	x uniformResourceI- dentifier [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	-
		accessMethod	x id-crossCertIndica- tion (see [V2G20-2604])	x id-crossCertIndica- tion (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 alphanu- meric string with a maximum length of 5 bytes as described here)	x “CROSS” (Syntax: An alphanu- meric 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

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
		algorithm	x id-Ed448	x id-Ed448
		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 CPS]	x [up to CPS]
	Subject	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) & "CPS"
	Subject- PublicKey- Info	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-authorityKey- Identifier	x / nc id-ce-authorityKey- Identifier
		keyIdentifier	x (see [V2G20-1851])	x (see [V2G20-1851])
		authorityCertIssuer	-	-

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	-
	Extensions	CRLDistributionPoints	(x) / nc id-ce-cRLDistributionPoints	(x) / nc id-ce-cRLDistributionPoints	(x) / nc id-ce-cRLDistributionPoints

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 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
		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 uniformResourceI- dentifier [6]	x uniformResourceI- dentifier [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	-
		accessMethod	x id-crossCertIndica- tion (see [V2G20-2604])	x id-crossCertIndica- tion (see [V2G20-2604])	-
		accessLocation	x	x	-
		generalName	x otherName [0]	x otherName [0]	-

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.