SLOVENSKI STANDARD
SIST EN ISO 15118-20:2022/oprA1:2025

01-februar-2025

Cestna vozila - Komunikacijski vmesnik med vozilom in omrežjem - 20. del: Zahteve za omrežno in aplikacijsko plast druge generacije - Dopolnilo A1 (ISO 15118-20:2022/DAmd1:2024)

Road vehicles - Vehicle to grid communication interface - Part 20: 2nd generation network layer and application layer requirements - Amendment 1: AC DER service, MCS service, and improved security concept (ISO 15118-20:2022/DAmd1:2024)

Straßenfahrzeuge - Kommunikationsschnittstelle zwischen Fahrzeug und Ladestation - Teil 20: Anforderungen der 2. Generation an das Netzwerk- und Anwendungsprotokoll - Ergänzung 1 (ISO 15118-20:2022/DAmd 1:2024)

Véhicules routiers - Interface de communication entre véhicule et réseau électrique - Partie 20: Exigences des couches réseau et application de 2ème génération - Amendement 1: Titre manque (ISO 15118-20:2022/DAmd1:2024)

Ta slovenski standard je istoveten z: **EN ISO 15118-20:2022/prA1:2024**

ICS:

35.100.05	Večslojne uporabniške rešitve	Multilayer applications
43.040.15	Avtomobilska informatika. Vgrajeni računalniški sistemi	Car informatics. On board computer systems

SIST EN ISO 15118-20:2022/oprA1:2025 **en,fr,de**

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

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

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:

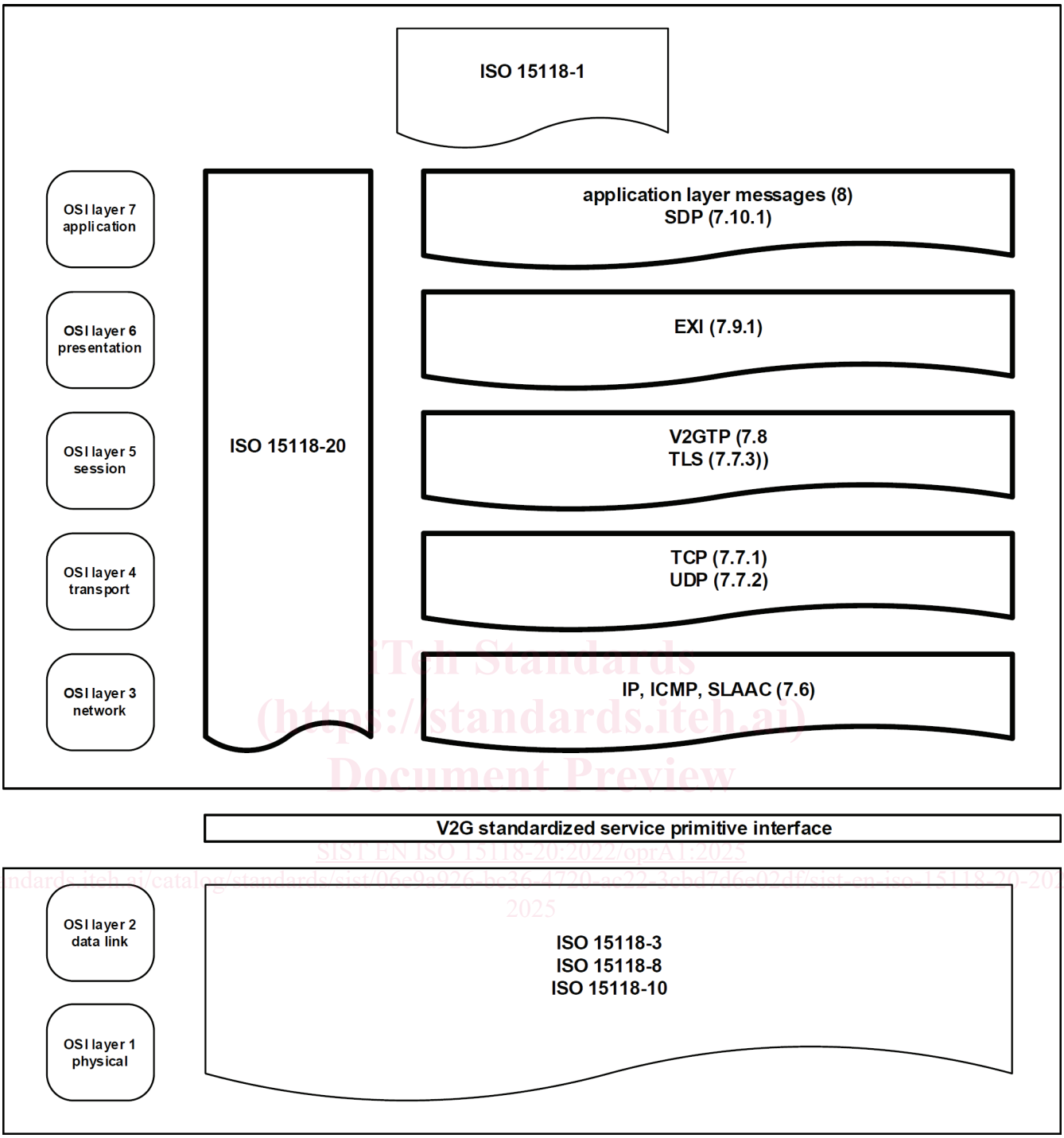


Figure 2 — Vehicle to grid communication document overview

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

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

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

[V2G20-3003] OCSP signer certificate used to sign the OCSP response for contract certificate status shall be generated using a certificate chain that uses either the same 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] OCSP signer certificate used to sign the OCSP response for vehicle certificate status shall be generated using a certificate chain that uses either the same OEM Root CA certificate or the same V2G Root CA certificate as the trust anchor as the vehicle certificate whose status is being checked. Refer to Figure 7 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of certificate structure. Refer to Annex B for details of the certificate profile.

Replace NOTE 10 with:

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

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

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

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

Clause 7.3.4

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

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:

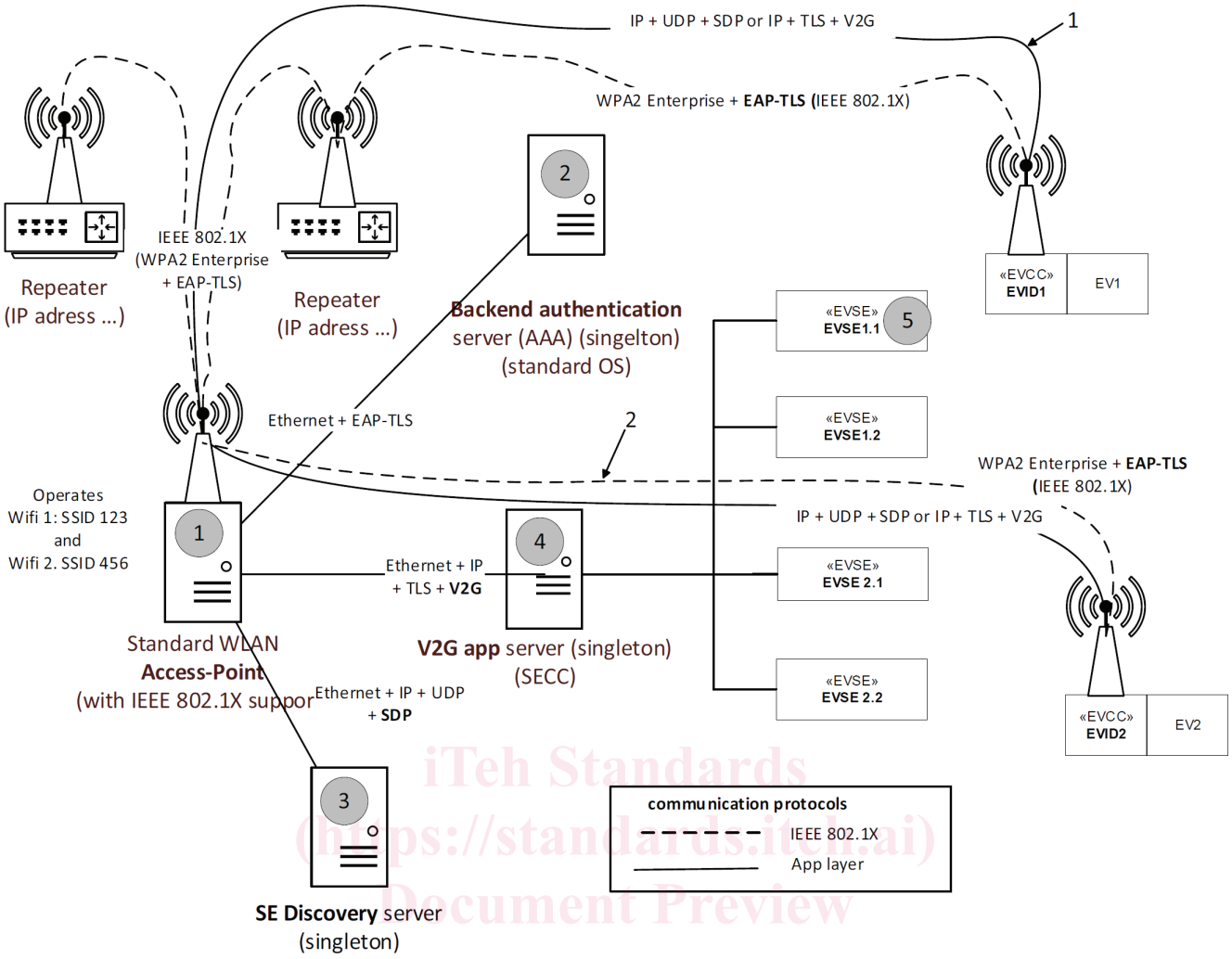
ISO 15118-3, ISO 15118-8, and ISO 15118-10 define additional details on data link layer to be covered.

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.