

DIN EN ISO 15118-20



ICS 43.120

Entwurf

Einsprüche bis 2022-04-18
Ersatz für
E DIN EN ISO 15118-2:2018-12

**Straßenfahrzeuge –
Kommunikationsschnittstelle zwischen Fahrzeug und Ladestation –
Teil 20: 2. Generation Anforderungen an das Netzwerk- und
Anwendungsprotokoll (ISO/FDIS 15118-20:2022);
Englische Fassung prEN ISO 15118-20:2022, nur auf CD-ROM**

Road vehicles –
Vehicle to grid communication interface –
Part 20: 2nd generation network and application protocol requirements
(ISO/FDIS 15118-20:2022);
English version prEN ISO 15118-20:2022, only on CD-ROM

Véhicules routiers –
Interface de communication entre véhicule et réseau électrique –
Partie 20: Exigences des couches réseau et application de 2ème génération
(ISO/FDIS 15118-20:2022);
Version anglaise prEN ISO 15118-20:2022, seulement en CD-ROM

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2022-02-18 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

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

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

DIN-Normenausschuss Automobiltechnik (NAAutomobil) Gesamtumfang 525 Seiten

Nationales Vorwort

Dieses Dokument (prEN ISO 15118-20:2022) wurde vom Technischen Komitee ISO/TC 22 „Road vehicles“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 301 „Straßenfahrzeuge“, dessen Sekretariat von AFNOR (Frankreich) gehalten wird, erarbeitet.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 052-00-31 AA „Datenkommunikation“ des DIN-Normenausschusses Automobiltechnik (NAAutomobil).

Dieses Dokument ist derzeit zur parallelen Abstimmung vorgelegt.

Dieses Dokument enthält unter Berücksichtigung des DIN-Präsidialbeschlusses 1/2004 nur die englische Originalfassung von EN ISO 15118-20.

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

ISO 15118-1	siehe	DIN EN ISO 15118-1
ISO 15118-2:2014	siehe	DIN EN ISO 15118-2:2016-08
ISO 15118-3:2015	siehe	DIN EN ISO 15118-3:2016-08
ISO 15118-8	siehe	DIN EN ISO 15118-8

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

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

Dieser Teil der Normenreihe legt die 2. Generation von allgemeinen Anforderungen an die Kommunikationsschnittstelle sowie die sicherheitsrelevanten Funktionen fest, die auf den Anwendungsfällen von DIN EN ISO 15118-1:2019-08 basieren.

Nationaler Anhang NA (informativ)

Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: unter <http://www.iso.org/obp>

3.1

Zugriffspunkt

AP, en: access point

Gerät mit drahtloser Kommunikation, das dem Nutzer erlaubt, sich mit anderen drahtlosen, oder verdrahteten Kommunikationsgeräten zu verbinden

3.2

Autorisierungsmodus

en authorization mode

Authentifizierung oder Autorisierung des Benutzerkontos

Anmerkung 1 zum Begriff: Autorisierungsmodus bezieht sich auf *EIM* (3.17) und *PnC* (3.41).

3.3

automatisches Pantograf-Verbindungsgerät

ACDP, en: automatic connection device pantograph

Komponenten, die den automatischen Verbindungs- und Öffnungsprozess für den kabelgebundenen Energietransfer zwischen einem Elektrofahrzeug (en: electric vehicle, EV) und der EV-Versorgungseinrichtung (en: electric vehicle supply equipment, EVSE) über einen Pantografen unterstützen

3.4

Grundladen

BC, en: basic charging

PWM-basiertes Laden

Anmerkung 1 zum Begriff: Nach ISO/IEC 11889-1:2015, Anhang A.

3.5

Zertifikat

en certificate

elektronisches Dokument, das eine digitale Signatur verwendet, um einen öffentlichen Schlüssel mit einer Identität zu verbinden

Anmerkung 1 zum Begriff: Die ISO 15118 Normenreihe beschreibt mehrere Zertifikate, welche unterschiedliche Zwecke abdecken [z. B. Vertragszertifikate inklusive *EMAID* (3.19) und *OEM* (3.36) Versorgungszertifikate].

3.6

Ladegrenzen

en charging limits

Menge technischer Bedingungen, die während einer *Dienstsitzung* (3.50) ausgehandelt werden

BEISPIEL Spannung, Strom, Energie, Leistung, usw.

3.7

Lademodus

en charging session

Sammlung von Ladetransaktionen an einem Ladepunkt, die nur auf das Laden eines Elektrofahrzeuges bezogen sind, das einem bestimmten Kunden in einem bestimmten Zeitfenster mit einem eindeutigen Bezeichner zugeordnet ist

Anmerkung 1 zum Begriff: Der Lademodus ist Untermenge der *Dienstsitzung* (3.50).

3.8

Ladestationsbetreiber

CSO, en: charging station operator

zweitrangiger Akteur, der für die Installation und den Betrieb einer Ladeinfrastruktur (inklusive Ladeplätze), sowie für das Management von Elektrizität verantwortlich ist, um die geforderten Energieübertragungsdienste bereitzustellen

Anmerkung 1 zum Begriff: Der Begriff Ladestationsbetreiber wird auch in anderen ISO 15118-Dokumenten verwendet. Dieser Begriff wird nicht für Schutzmarken empfohlen.

3.9

Kommunikationssitzung

en communication session

Zeitsequenz, während der die *EVCC* (3.21) und *SECC* (3.47) interaktiv digitale Informationen austauschen, um das Laden und Entladen der EV-Batterie zu steuern

Anmerkung 1 zum Begriff: Eine Kommunikationssitzung kann mehrere Male angehalten und fortgesetzt werden. Die Kommunikationssitzung umfasst keine oder mehrere Energieübertragungsperioden.

3.10

Kommunikationsstartzeitgeber

en communication setup timer

Zeitgeber (3.61), der die Zeit zwischen dem Aufbau der TLS-Verbindung und dem Empfang von *SessionSetupRes* in der *EVCC* (3.21) überwacht

3.11

Vertragszertifikat

en contract certificate

Zertifikat (3.5), welches für die *EVCC* (3.21) von einer nachrangigen Zertifikatsbehörde (3.57) des *eMSP's* (3.20) ausgestellt wurde und in XML-Signaturen in den Anwendungsschichten verwendet wird, so dass die *SECC* (3.47) oder ein zweitrangiger Akteur die Signatur überprüfen kann, die von der *EVCC*, mit dem für das EV ausgestellte Vertragszertifikat, erstellt wurde

Anmerkung 1 zum Begriff: Der zweitrangige Akteur verwendet den *EMAID* (3.19), der Teil der Betreffzeile des Vertragszertifikates ist, um das EV für den Ladevorgang, basierend auf dem zugehörigen E-Mobilitätsvertrages des *eMSP's*, zu autorisieren.

3.12

Status Vorsteuerung

en control pilot state, CP state

Vorsteuerungsstatus gemäß der Vorsteuerungsfunktion nach IEC 61851-1

3.13

Berechtigungsnachweis

en credential

Teilinformation, welche die Identität einer Einheit bestätigt

3.14

Überkreuz-Zertifikat

en cross certificate

Zertifikat (3.5), welches den öffentlichen Schlüssel eines bestehenden Zertifikates einer Zertifikatsbehörde (en: certificate authority, CA) in einer Organisation (genannt Überkreuz-Zertifizierungsbehörde) beinhaltet, aber von einer Hauptzertifikatsbehörde (en: root CA) einer anderen Organisation (genannt Überkreuz-Zertifizierungsbehörde) gezeichnet wurde

Anmerkung 1 zum Begriff: Mit Überkreuz-Zertifizierung, kann eine Endgebilde, das nur einer Überkreuz-Hauptzertifikatsbehörde vertraut, eine Zertifikatskette, die von einer Hauptzertifikatsbehörde einer anderen Organisation ausgestellt wurde, durch ein Überkreuz-Zertifikat, das an die Kette angehängt wurde, bestätigen.

3.15

hervorgehobene Verschlüsselungsregeln

DER, en: distinguished encoding rules

Methode zur Verschlüsselung eines Datenobjektes, wie z. B. ein *X.509-Zertifikat* (3.5), welches digital gezeichnet, oder dessen Signatur verifiziert wurde

3.16

dynamischer Steuerungsmodus

en dynamic control mode

Steuerungsmodus für die Kommunikation

Anmerkung 1 zum Begriff: Weitere Informationen können in ISO 15118-1 gefunden werden.

Anmerkung 2 zum Begriff: Die *SECC* (3.47) steuert den Leistungsfluss und stellt der *EVCC* (3.21) Sollwerte zur Verfügung, dem er folgen sollte.

3.17

externes Identifikationsmerkmal

EIM, en: external identification means

Autorisierungsmerkmal, welches außerhalb dieses Dokumentes gehandhabt wird

3.18

Kryptographie mittels elliptischer Kurven

ECC, en: elliptic curve cryptography

Mechanismus zur Implementierung von Kryptographie mit öffentlichen Schlüsseln, basierend auf dem diskreten Logarithmus algebraischer Strukturen elliptischer Kurven

3.19

E-Mobilität-Authentifizierungsbezeichner

EMAID, en: eMobility account identifier

Vertragsidentifizierung für den Vertrag, der vom *eMSP* (3.20) ausgestellt ist, und von der *SECC* (3.47) oder einem zweitrangigen Akteur verwendet wird, um die Energieübertragung und bezogene Dienste (inklusive Abrechnung) zu ermöglichen

Anmerkung 1 zum Begriff: Der Begriff Vertragsbezeichner wird in diesem Dokument nicht mehr verwendet. Er wurde durch den Begriff EMAID ersetzt. Der Begriff ist aber aus Kompatibilitätsgründen mit ISO 15118-1 immer noch vorhanden.

3.20

E-Mobilitätsdienstanbieter

eMSP, en: eMobility service provider

Einheit, mit der der Kunde einen Vertrag für alle Dienste, die sich auf die Energieübertragung zum EV beziehen

Anmerkung 1 zum Begriff: Typischerweise beinhaltet der eMSP einige der anderen Akteure, wie lokale Betreiber oder Energielieferanten (en: electricity provider, EP), und hat eine enge Beziehung mit den Verteilnetzbetreibern und *Stromzählerbetreibern* (3.33). Ein *OEM* (3.36) oder Versorgungsunternehmen könnte diese Rolle ebenfalls erfüllen.

Anmerkung 2 zum Begriff: Der eMSP überprüft die *EMAIDs* (3.19) seiner Kunden, die er entweder von der Verrechnungsstelle des E-Mobilitätsbetreibers (en: e-mobility operator clearing house, EMOCH), anderen eMSPs oder lokalen Betreibern empfängt, mit denen der Kunde in Beziehung steht.

Anmerkung 3 zum Begriff: Der eMSP stellt EMAIDs für seine Kunden aus.

3.21

Kommunikationssteuerung Elektrofahrzeug

EVCC, en: electric vehicle communication controller

im Fahrzeug eingebautes System, welches die Kommunikation zwischen dem Fahrzeug und der *SECC* (3.47) umsetzt, um spezifische Funktionen zu unterstützen

Anmerkung 1 zum Begriff: Solche spezifischen Funktionen könnten z. B. die Steuerung von Ein- und Ausgangskanälen, Verschlüsselung oder die Datenübertragung zwischen Fahrzeug und SECC sein.

3.22

EV-Leistungsprofil

en EVpowerProfile

Zeitplan, welcher die Leistungsgrenzen zum Laden und Entladen der Batterie während einer Energieübertragungsperiode enthält

Anmerkung 1 zum Begriff: Siehe auch Begriff „Energieübertragungszeitplan“ in ISO 15118-1.

Anmerkung 2 zum Begriff: Im *dynamischen Steuerungsmodus* (3.16) wird eine Simulation aus EV-Sicht für das schnellste Ladeprofil beschrieben, um den EVMaximumEnergyRequest unter der Bedingung der Minimalwerte von EVSEMaximumChargePower und EVMaximumChargePower zu erreichen.

BEISPIEL Der Zeitplan wird basierend auf dem Zielwert, Verkaufstariftabelle und Netzzeitplaninformation unter Berücksichtigung der entsprechenden Strombegrenzungen berechnet, d. h. unter Verwendung des tiefsten Stromwertes.

3.23

Elektrofahrzeug-Ladeeinrichtungsbezeichner

EVSEID, en: electric vehicle supply equipment ID

eindeutige Bezeichnung der EVSE

3.24

Elektrofahrzeug-Ladeeinrichtung

EVSE, en: electric vehicle supply equipment

<kabelgebundene Leistungsübertragung> Stromleitungen, inklusive der Phase(n)-, Neutralleiter- und Schutzerdeleitungen, der EV-Steckvorrichtung, angeschlossene Stecker sowie alle weiteren Ausstattungen, Geräte, Steckdosen oder Apparate, die speziell für die Energielieferung vom örtlichen Kabelsatz zum EV installiert wurden, und die notwendige Kommunikation untereinander ermöglichen

3.25

Elektrofahrzeug-Ladeeinrichtung

EVSE, en: electric vehicle supply equipment

<induktive Leistungsübertragung> Off-board-Elektronik, welche die *SECC* (3.47), sowie ein oder mehrere Versorgungsgerät(e) umfasst, die von derselben *SECC* gesteuert werden

3.26

globale Adresse

en global address

IP-Adresse (3.28) mit uneingeschränktem Anwendungsbereich

3.27

übergeordnete Ladekommunikation

HLC-C, en: high level communication charging

Energieübertragungsphase während der *Dienstszitzung* (3.50)

3.28

IP-Adresse

en IP address

IP-Schicht-Bezeichner für eine Schnittstelle oder eine Menge von Schnittstellen

3.29

Link-lokale Adresse

en link-local address

IP-Adresse (3.28), die nur in einem Netz angewendet wird und dazu verwendet wird, benachbarte Schnittstellen im selben Netz anzusprechen

3.30

maximale Übertragungseinheit

MTU, en: maximum transfer unit

maximale Größe (in Bytes) der größten Protokolldateneinheit, welche die Sicherungsschicht weiterleiten kann

3.31

Botschaftsmenge

en message set

Menge von *V2G-Kommunikationsbotschaften* (3.66) und Parameter für die *EVCC* (3.21) oder *SECC* (3.47), welche ein oder mehrere Anwendungselement(e) abdeckt(abdecken)

3.32

Botschaftszeitgeber

en message timer

Zeitgeber (3.61), der den Austausch eines Anfrage-Antwort-Paares überwacht

3.33

Stromzähler

en meter

analoges Gerät, das fähig ist, die verbrauchte Energiemenge zu messen und zu überwachen

3.34

Multiplexkommunikation

MC, en: multiplex communication

Austausch mehrerer Botschaften mit unterschiedlichen Nutzdatentypen zwischen der *EVCC* (3.21) und der *EVSE* (3.47) über die *V2GTP*-Verbindung (3.68)

3.35

Knoten

en node

Gerät, welches IPv6 implementiert

3.36

Originalgerätehersteller

OEM, en: original equipment manufacturer

Hersteller, der Produkte oder Komponenten produziert, die von einer Firma eingekauft werden und unter dem Markennamen der Firma verkauft werden

Anmerkung 1 zum Begriff: OEM bezieht sich auf eine Firma, die der ursprüngliche Hersteller des Produkts ist.

Anmerkung 2 zum Begriff: Bezogen auf Automobilteile, bezeichnet OEM ein Austauschteil, das vom Hersteller des Originalteils gemacht wurde.

3.37

Versorgungszertifikat der OEM

en OEM provisioning certificate

Zertifikat (3.5), welches für die *EVCC* (3.21) vom *OEM* (3.36) ausgestellt wurde, damit die Bereitstellung eines *Vertragszertifikates* (3.11) ermöglicht wird

Anmerkung 1 zum Begriff: Es wird in sicherer Art und Weise von einem zweitrangigen Akteur angefragt und empfangen, um die *EVCC* eindeutig zu identifizieren.

3.38

PE-Zertifikat

en PE certificate

Blattzertifikat (3.5), welches in *PE* (3.42) für eine *private SECC* (3.43) von einer Hauptzertifikatsbehörde in privater Umgebung, oder optional von einer Unterzertifikatsbehörde in privater Umgebung, ausgestellt wurde und für TLS verwendet wird, sodass die *EVCC* (3.21) die Authentizität der privaten *SECC* überprüfen kann

3.39

PE-EVSE

EVSE, die in einer *privaten Umgebung* (3.42) betrieben wird, und eine *private SECC* (3.43) beinhaltet, oder von einer gesteuert wird

3.40

Durchführungszeit

en performance time

nicht-funktionale Zeitanforderung, die die Zeit festlegt, die eine *V2G-Einheit* (3.65) während der Ausführung bestimmter Funktionalitäten nicht überschreiten sollte

Anmerkung 1 zum Begriff: Dies ist ein fester Zeitwert.

3.41

parken und laden

PnC, en: park and charge

Authentifizierungsmechanismus, der im EV gespeicherte *Zertifikate* (3.5) verwendet und keinerlei Interaktion des Nutzers verlangt

3.42

private Umgebung

PE, en: private environment

Gebiet privater Verantwortlichkeit mit räumlichem Zugang, der auf eine kleine Anzahl von Fahrzeugen beschränkt ist

3.43

private SECC

SECC (3.47), die in einer *privaten Umgebung* (3.42) betrieben wird und ein *PE-Zertifikat* (3.38) verwendet

Anmerkung 1 zum Begriff: *PE* (3.42) impliziert normalerweise geringe Security. In den meisten Fällen gelten *SECC*-Anforderungen auch für eine private *SECC*. In einigen spezifischen Fällen können Anforderungen für *SECC*- und private *SECC* voneinander abweichen. Solche Fälle und Anforderungen werden als solche gekennzeichnet.

3.44

öffentliche SECC

en public *SECC*

SECC (3.47), die in einer öffentlichen Umgebung betrieben wird und ein *PE-Zertifikat* (3.38) verwendet

3.45

Anfrage-Antwort-Botschaftspaar

en request-response message pair

Anfragebotschaft mit entsprechender Antwortbotschaft

3.46

Anfrage-Antwort-Botschaftssequenz

en request-response message sequence

vordefinierte Sequenz von *Anfrage-Antwort-Botschaftspaaren* (3.45)

3.47

Kommunikationssteuerung Ladeeinrichtung

SECC, en: supply equipment communication controller

Entität, welche die Kommunikation für eine oder mehrere *EVCCs* (3.21) umsetzt und welche sich mit zweitrangigen Akteuren austauschen kann

Anmerkung 1 zum Begriff: Funktionen einer Kommunikationssteuerung Ladeeinrichtung können Ein- oder Ausgänge, Datenverschlüsselung oder die Datenübertragung zwischen Fahrzeug und *SECC* steuern.

3.48

SECC-Zertifikat

en SECC certificate

Blattzertifikat (3.5), welches für die *SECC* (3.47) von einer zweiten Unterzertifikatsbehörde (en: sub-CA2) des *CSOs* (3.8) ausgestellt wurde, welches für TLS derart verwendet wird, dass die *EVCC* (3.21) die Authentizität des *SECC* verifizieren kann

3.49

Sequenzzeitgeber

en sequence timer

Zeitgeber (3.61), der eine *Anfrage-Antwort-Botschaftssequenz* (3.46) überwacht

3.50

Dienstsitzung

en service session

Sammlung von Diensten zu einem Ladepunkt, hauptsächlich bezogen auf das Laden des EVs, welches einem spezifischen Kunden in einem spezifischen Zeitfenster mit einem eindeutigen Bezeichner zugeteilt ist

Anmerkung 1 zum Begriff: *Lademodus* (3.7) und kalbellose Leistungsübertragungssitzung sind Arten von Dienstsitzungen.

3.51

geplanter Steuerungsmodus

en scheduled control mode

Steuerungsmodus für die Kommunikation

Anmerkung 1 zum Begriff: Weitere Informationen können in ISO 15118-1 gefunden werden.

Anmerkung 2 zum Begriff: Die *EVCC* (3.21) und die *SECC* (3.47) verhandeln ein Leistungsprofil zum Zwecke des Ladens und Entladens.

3.52

Zeitplan Neuverhandlung

en schedule renegotiation

Botschaftsaustausch zur Erneuerung der Übereinkunft des Ladezeitplans zwischen *EVCC* (3.21) und *SECC* (3.47) während einer *V2G-Kommunikationssitzung* (3.64) durch die Neuübertragung der Parameter Zeitplan und *EVLeistungsProfil* (3.22)

3.53

Station

STA, en: station

logische Einheit, die eine einzelne adressierbare Instanz einer Medienzugriffssteuerung und Schnittstelle der physikalischen Schicht zum drahtlosen Medium darstellt, aber nicht als *Zugriffspunkt* (3.1) agiert

3.54

SECC-Entdeckungsprotokoll Client

en SDP Client

V2G-Einheit (3.65), die den *SDP-Server* (3.55) nutzt, um Konfigurationsinformationen über die *SECC* (3.47) zu bekommen, um auf diese zugreifen zu können

3.55

SECC-Entdeckungsprotokoll Server

en SDP Server

V2G-Einheit (3.65), die Konfigurationsinformationen für den Zugriff auf die *SECC* (3.47) liefert

3.56

intelligenter Stromzähler

en smart meter

Gerät, das fähig ist, die verbrauchte oder generierte Energiemenge zu messen und zu überwachen

Anmerkung 1 zum Begriff: In diesem Fall während des EV *Lademodus* (3.7).

Anmerkung 2 zum Begriff: Die Werte für aktive/reaktive Energie, aktive/reaktive Leistung, Strom, Leistungsfaktor, basierend auf dem Zeitfenster, können aufgezeichnet werden. Die Werte werden fernüberwacht, so dass sie programmiert werden können, um die Leistung zu steuern (z. B. zu reduzieren oder zu modulieren). Darüber hinaus können die Werte die Informationen mit DSO und anderen Geräten auf der Grundlage der SPS-Kommunikation teilen.

3.57

Untertzertifikatsbehörde

en Sub-CA

untergeordnete Zertifikatsbehörde, die z. B. *SECC-Zertifikate* (3.48) und/oder im Auftrag der Hauptzertifikatsbehörde *Vertragszertifikate* (3.11) ausstellt, wie z. B. *V2G-Hauptzertifikate* (3.70) oder Hauptzertifikate für E-Mobilität Dienstanbieter (letzteres nur für Vertragszertifikate)

Anmerkung 1 zum Begriff: Die Fähigkeit zur Ausstellung der Zertifikate wird von der Hauptzertifikatsbehörde übertragen und die Hauptzertifikatsbehörde kann diese Übertragung an die Untertzertifikatsbehörde jederzeit rückgängig machen.

3.58

Untertzertifikatsbehördenzertifikat

en Sub-CA certificate

von der *Untertzertifikatsbehörde* (3.57) ausgestelltes *Zertifikat* (3.5)

3.59

TCP-Daten

en TCP_DATA

Socket-Schnittstelle für einen Datentransfer basierend auf einer TCP-Verbindung

3.60

Zeitüberschreitung

en timeout

Zeitanforderung zur Festlegung der Zeit, während der eine *V2G-Einheit* (3.65) überwacht, ob im Kommunikationssystem ein bestimmtes Ereignis auftritt

Anmerkung 1 zum Begriff: Wenn die festgelegte Zeit überschritten wird, initiiert die betroffene *V2G-Einheit* (3.65) die entsprechende Fehlerbehandlung. Dies ist ein festgelegter Zeitwert.

3.61

Zeitgeber

en timer

Gerät oder Teil der Software zur Zeitmessung in einer Implementierung

Anmerkung 1 zum Begriff: Abhängig vom spezifischen Anwendungsfall, wird ein Zeitgeber auch zum Anstoßen bestimmter Systemereignisse verwendet.

3.62

Fahrzeug Zertifikat

en vehicle certificate

Blattzertifikat (3.5), welches von einem *OEM* (3.36) für eine *EVCC* (3.21) oder *V2G* (3.63) ausgestellt wurde und für TLS verwendet wird, sodass die *SECC* (3.47) die Authentizität der EVCC überprüfen kann

Anmerkung 1 zum Begriff: Dieses Zertifikat wird außerdem für die Bindung zwischen zwei verschiedenen TLS-Sitzungen verwendet, die zur selben V2G-Sitzung der SECC gehören.

3.63

Fahrzeug-zu-Ladesäule

V2G, en: vehicle to grid

Interaktion zum Verbinden des EVs mit der elektrischen Ladesäule, inklusive Laden sowie Entladen und bidirektionale Kommunikationsschnittstelle

Anmerkung 1 zum Begriff: Der erste Teil dieser Definition ist vom Anwendungsbereich der V2G-Expertenarbeitsgruppe, SGIP, NIST extrahiert.

3.64

V2G-Kommunikationssitzung

en V2G communication session

Zuordnung von zwei spezifischen V2G-Einheiten für den Austausch von *V2G-Botschaften* (3.66)

3.65

V2G-Einheit

en V2G entity

primärer Akteur, der an der V2G-Kommunikation beteiligt ist

Anmerkung 1 zum Begriff: Primäre Akteure können der *EVCC* (3.21) oder *SECC* (3.47) sein.

3.66

V2G-Botschaft

en V2G message

Botschaft, die in der Anwendungsschicht ausgetauscht wird

Anmerkung 1 zum Begriff: Siehe Abschnitt 8.

3.67

V2G-Konfiguration

en V2G setup

Konfigurationsphase für den V2G-Botschaftsaustausch

3.68

V2G-Übertragungsprotokoll

V2GTP, en: V2G transfer protocol

Kommunikationsprotokoll für die Übertragung von *V2G-Botschaften* (3.66) zwischen zwei V2GTP-Einheiten

3.69

V2GTP-Einheit

en V2GTP entity

V2G-Einheit (3.65), die das *V2G-Übertragungsprotokoll* (3.68) unterstützt

3.70

V2G-Hauptzertifikatsbehörde

en V2G root CA

Zertifikatsbehörde (CA), welche *Untertzertifikatsbehörden* (3.57) Zertifikate an Untertzertifikatsbehörden ausstellt

Anmerkung 1 zum Begriff: Diese Untertzertifikatsbehörden sind dann angewiesen, entweder Zertifikate an eine zweite Untertzertifikatsbehörde (Sub-CA2) auszustellen oder direkt Blattzertifikate, wie *Vertragszertifikate* (3.11) oder *SECC-Zertifikate* (3.48), auszustellen

3.71

V2G-Hauptzertifikat

en V2G root certificate

Zertifikat, welches von der *V2G-Hauptzertifikatsbehörde* (3.70) ausgestellt wurde

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN ISO 15118-1, *Straßenfahrzeuge — Kommunikationsschnittstelle zwischen Fahrzeug und Ladestation — Teil 1: Allgemeine Informationen und Festlegungen der Anwendungsfälle*

DIN EN ISO 15118-2:2016-08, *Straßenfahrzeuge — Kommunikationsschnittstelle zwischen Fahrzeug und Ladestation — Teil 2: Anforderungen an das Netzwerk- und Anwendungsprotokoll (ISO 15118-2:2014); Englische Fassung EN ISO 15118-2:2016, nur auf CD-ROM*

DIN EN ISO 15118-3:2016-08, *Straßenfahrzeuge — Kommunikationsschnittstelle zwischen Fahrzeug und Ladestation — Teil 3: Anforderungen an physikalische- und Datenverbindungsschnittstelle (ISO 15118-3:2015); Englische Fassung EN ISO 15118-3:2016*

DIN EN ISO 15118-8, *Straßenfahrzeuge — Kommunikationsschnittstelle zwischen Fahrzeug und Ladestation — Teil 8: Anforderungen an Bitübertragungs- und Sicherungsschicht für die drahtlose Kommunikation*

— Leerseite —

Contents

Page

1	Scope	1
2	Normative references	1
3	Terms and definitions	4
4	Abbreviated terms	11
5	Conventions	14
5.1	Definition of OSI based services	14
5.2	Requirement structure	14
5.3	Usage of references	15
5.4	Notation used for XML schema diagrams.....	15
6	Document overview.....	15
7	Basic requirements for V2G communication	16
7.1	General information	16
7.2	Service primitive concept of OSI layered architecture.....	17
7.2.1	Overview.....	17
7.2.2	Syntax of service primitives	17
7.3	Security concept.....	18
7.3.1	General	18
7.3.2	Certificate and key management	20
7.3.3	Number of root certificates and root validity	32
7.3.4	Support and application of TLS	34
7.3.5	Firewall	34
7.3.6	Protection of the cryptographic keys	35
7.3.7	Random number generation	36
7.4	V2G communication states and data link handling	38
7.5	Data link layer	42
7.5.1	Data link layer security for WLAN.....	43
7.6	Network link layer.....	48
7.6.1	General	48
7.6.2	Applicable RFCs, limitations and protocol parameter settings.....	48
7.6.3	IP addressing	50
7.7	Transport layer	50
7.7.1	Transmission control protocol (TCP).....	50
7.7.2	User datagram protocol (UDP)	51
7.7.3	Transport layer security (TLS)	52
7.8	V2G transfer protocol.....	75
7.8.1	General information	75
7.8.2	Supported ports.....	75
7.8.3	Protocol data unit.....	76
7.9	Presentation layer	80
7.9.1	XML and efficient XML interchange (EXI)	80
7.9.2	Message security.....	83
7.10	Application layer.....	105
7.10.1	SECC discovery protocol	106
8	Application layer messages	117
8.1	General information and definitions.....	117
8.2	Protocol handshake definition	117
8.2.1	Handshake sequence.....	118
8.2.2	Message definition supportedAppProtocolReq and supportedAppProtocolRes	119
8.2.3	Semantics description supportedAppProtocol messages	120
8.2.4	Message examples	121
8.3	V2G message definition.....	122
8.3.1	Overview.....	122
8.3.2	General	123
8.3.3	Header definition	123
8.3.4	Request and response definitions.....	126

8.3.5	Complex data types	215
8.4	Service selection	320
8.4.1	General	320
8.4.2	General description of configuration parameters	321
8.4.3	Selection of service and service parameters	322
8.5	V2G communication timing	330
8.5.1	Overview	330
8.5.2	Common	330
8.5.3	DC service	331
8.5.4	Message sequence and communication session	331
8.5.5	Session setup and ready to charge	337
8.5.6	V2G message synchronization for AC and DC with IEC 61851-1 signalling	341
8.5.7	V2G message synchronization with IEC 61980-2 signalling for WPT	348
8.6	Message sequencing and error handling	348
8.6.1	Overview	348
8.6.2	Basic definitions for error handling	348
8.6.3	ResponseCode handling	349
8.6.4	Request-response message sequence requirements	359
8.6.5	Multiplexed communication	383
8.6.6	Message sequence diagrams	385
Annex A	(normative) Schema definition	391
Annex B	(normative) Certificate profiles	392
B.1	Overview	392
B.2	General	395
B.2.1	Mandatory versus optional	395
B.2.2	Critical versus non-critical	397
B.2.3	Common requirements for all certificate profiles	399
B.3	V2G root CA certificate profiles	400
B.3.1	Based on curves as defined by [V2G20-2674]	400
B.3.2	Based on curves as defined by [V2G20-2319]	401
B.4	Charge point operator certificate profiles	403
B.4.1	Based on curves as defined by [V2G20-2674]	403
B.4.2	Based on curves as defined by [V2G20-2319]	405
B.4.3	Common requirements for charge point operator certificate profiles	406
B.5	Certificate provisioning service certificate profiles	407
B.5.1	Based on curves as defined by [V2G20-2674]	407
B.5.2	Based on curves as defined by [V2G20-2319]	408
B.5.3	Common requirements for certificate provisioning service certificate profiles	410
B.6	e-Mobility service provider certificate profiles	410
B.6.1	Based on curves as defined by [V2G20-2674]	410
B.6.2	Based on curves as defined by [V2G20-2319]	413
B.6.3	Common requirements for e-mobility service provider certificate profiles	416
B.7	OEM provisioning certificate profiles	418
B.7.1	Based on curves as defined by [V2G20-2674]	418
B.7.2	Based on curves as defined by [V2G20-2319]	421
B.7.3	Common requirements for OEM provisioning certificate profiles	424
B.8	Vehicle certificate profiles	425
B.8.1	Based on curves as defined by [V2G20-2674]	425
B.8.2	Based on curves as defined by [V2G20-2319]	427
B.8.3	Common requirements for vehicle certificate profiles	429
B.9	Cross certificate & OCSP signer certificate profiles	430
B.9.1	Based on curves as defined by [V2G20-2674]	430
B.9.2	Based on curves as defined by [V2G20-2319]	432
B.9.3	Common requirements for cross certificate & OCSP signer certificate profiles	434
B.10	Private environment certificate profiles	435
B.10.1	Based on curves as defined by [V2G20-2674]	435
B.10.2	Based on curves as defined by [V2G20-2319]	437
B.10.3	Common requirements for private environment certificate profiles	439
Annex C	(normative) Specification of identifiers	441

C.1	e-Mobility authentication identifier (EMAID).....	441
C.1.1	EMAID syntax.....	441
C.2	Provisioning certificate identifier (PCID)	441
C.2.1	PCID syntax.....	441
C.2.2	PCID semantics	442
C.3	Supply equipment communications controller identifier (SECCID)	442
C.3.1	SECCID syntax.....	442
C.3.2	SECCID semantics	443
C.4	Electric vehicle supply equipment ID (EVSEID)	444
C.4.1	EVSEID syntax	444
C.5	Electric vehicle communication controller ID (EVCCID)	444
C.5.1	EVCCID syntax.....	444
C.5.2	EVCCID semantics	445
C.6	Calculation of the check digit	445
Annex D	(informative) ACDP	447
D.1	Coordinate system definition for ACDP with inverted pantograph	447
D.1.1	Coordinate system definitions.....	447
Annex E	(informative) Basic PPD for interoperability	449
E.1	Overview.....	449
E.2	RFID implementation (recommended)	449
E.2.1	Functional description	449
Annex F	(informative) Message sequencing for renegotiation	453
F.1	Overview.....	453
F.2	Renegotiation after resuming a V2G communication session	453
Annex G	(informative) Association of VAS client to V2G session.....	455
Annex H	(informative) Application of certificates.....	457
H.1	General information	457
H.1.1	Overview.....	457
H.1.2	Demands of the OEM	458
H.1.3	Demands of the secondary actors.....	458
H.1.4	Rationale for decisions in this document	459
H.1.5	Cross certification	460
H.1.6	Examples of the resulting certificate structure	464
H.2	Simplified certificate management in private environment	473
H.2.1	Overview.....	473
H.2.2	Solution for private environments.....	476
H.2.3	Security considerations of using private environment credentials	480
H.3	Solution for emergency and disaster situations	480
H.4	Use of OEM provisioning certificates.....	481
H.5	Offline contract certificate installation.....	481
H.5.1	Processes.....	482
H.6	Risks of root CA compromise.....	483
H.7	Security appliances and their associated certificates.....	483
Annex I	(informative) Precision of measurements and tolerances	491
Annex J	(informative) Absolute pricing examples	493
J.1	Overview.....	493
J.2	Simple examples	493
J.2.1	Parking fee only	493
J.2.2	Energy fee only.....	493
J.2.3	Energy and taxes.....	494
J.2.4	Minimum and maximum cost	494
J.3	Less simple examples.....	495
J.3.1	Different rates for different days.....	495
J.3.2	Different rates for different power levels	496
J.3.3	Different rates for different power levels including reverse power	496
J.3.4	Overstay after charging finished	497
J.3.5	Stacked prices	498

Bibliography 501

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC 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) or the IEC list of patent declarations received (see <https://patents.iec.ch>).

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. In the IEC, see www.iec.ch/understanding-standards.

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

A list of all parts in the ISO 15118-20 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

Introduction

The pending energy crisis and necessity to reduce greenhouse gas emissions started in the former century has led the vehicle manufacturers to a very significant effort to reduce the energy consumption of their vehicles up to the present. As countermeasures to this continuous problem, they developed vehicles partly or completely propelled by electric power and launched them into the market. Those vehicles will reduce the dependency on oil, improve the global energy efficiency and reduce the total CO₂ emissions for road transportation if the electricity is produced from renewable sources. To charge electricity to the batteries of such vehicles, a specific charging infrastructure is required.

Much of the standardization work on dimensional and electrical specifications of the charging infrastructure for electric vehicles and the vehicle interface were treated in the relevant ISO or IEC groups. However, the standardization work about direct information transfer between the electric vehicle and the charging infrastructure was not enough, and it was assigned to the ISO 15118 series to treat the subject sufficiently.

Such communication is necessary for the optimization of energy resources and energy production systems. With it electric vehicles can be connected to the supply network and communicate the most economic or most energy efficient way for charging/discharging. It is also required to develop efficient and convenient billing systems in order to cover the resulting payments. The necessary communication channel can serve in the future to contribute to the stabilization of the supply network as well as to support additional information services required to operate electric vehicles efficiently and economically.

After the standardization work of the first basic smart charging was completed, more standardization work for further evolved functions and high energy efficiency was continuously requested again.

It includes:

- improved charge methods that reduces efforts and agonies of the charging operation;
- extended functions for the electric vehicles to be utilized as distributed energy resources, which enable smoothing of the electricity load of the supply network for higher energy efficiency and also provide power back to the grid;
- information services for the user with higher added value and new convenience.

As for the communication system, the next evolution will be expected to realize these new applications.

Road vehicles — Vehicle to grid communication interface —

Part 20:

Network and application protocol requirements

1 Scope

This document specifies the communication between the electric vehicle (EV), including battery electric vehicle (BEV) and plug-in hybrid electric vehicle (PHEV), and the electric vehicle supply equipment (EVSE). The application layer messages defined in this document are designed to support the electricity power transfer between an EV and an EVSE.

This document defines the communication messages and sequence requirements for bidirectional power transfer.

This document furthermore defines requirements of wireless communication for both conductive charging and wireless charging as well as communication requirements for automatic connection device and information services about charging and control status.

The purpose of this document is to detail the communication between an electric vehicle communication controller (EVCC) and a supply equipment communication controller (SECC). Aspects are specified to detect a vehicle in a communication network and enable an Internet Protocol (IP) based communication between the EVCC and the SECC (see Figure 1).

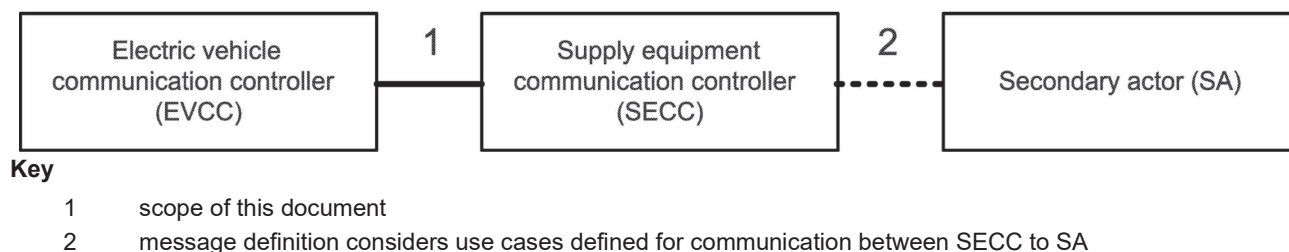


Figure 1 — Communication relationship among the EVCC, SECC and SA

This document defines messages, data model, XML/EXI-based data representation format, usage of V2GTP, TLS, TCP and IPv6. These requirements belong to the 3rd until the 7th OSI layer model. In addition, the document describes main service sequences of conductive charging, wireless power transfer and bidirectional power transfer, and how data link layer services can be accessed from an OSI layer 3 perspective.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 3780, *Road vehicles – World Manufacturer Identifier (WMI) code*

ISO 4217, *Codes for the representation of currencies*

ISO 15118-2:2014, *Road vehicles — Vehicle to grid communication interface — Part 2: Network and application protocol requirements*

ISO 15118-3:2015, *Road Vehicles — Vehicle to grid communication interface — Part 3: Physical and data link layer requirements*

ISO 15118-8, *Road Vehicles — Vehicle to grid communication interface — Part 8: Physical and data link layer requirements for wireless communication*

ISO 19363:2020, *Electrically propelled vehicles—Magnetic field wireless power transfer—Safety and interoperability requirements*

ISO/IEC 11889-1:2015, *Information technology — Trusted platform module library — Part 1: Architecture*

IEC 61851-1:2017, *Electric vehicle conductive charging system — Part 1: General requirements*

IEC 61851-23-1:2014, *Electric vehicle conductive charging system - Part 23-1: DC Charging with an automatic connection system*

IEC 61980-2, *Electric vehicle wireless power transfer (WPT) systems - Part 2: Specific requirements for communication between electric road vehicle (EV) and infrastructure*

IEC 63119-2, *Information exchange for Electric Vehicle charging roaming service — Part 2: Use cases*

EN 50696:2021, *Contact interface for automated connection devices (ACD)*

IETF RFC 768, *User Datagram Protocol* (August 1980)

IETF RFC 793, *Transmission Control Protocol - DARPA Internet Program - Protocol Specification* (September 1981)

IETF RFC 2865, *Remote Authentication Dial In User Service (RADIUS)* (June 2000)

IETF RFC 2866, *RADIUS Accounting* (June 2000)

IETF RFC 3122, *Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification* (June 2001)

IETF RFC 3579, *RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)* (September 2003)

IETF RFC 3748, *Extensible Authentication Protocol (EAP)* (June 2004)

IETF RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax* (January 2005)

IETF RFC 4291, *IP Version 6 Addressing Architecture* (February 2006)

IETF RFC 4429, *Optimistic Duplicate Address Detection (DAD) for IPv6* (April 2006)

IETF RFC 4443, *Internet Control Message Protocol (ICMP v6) for the Internet Protocol version 6 (IPv6) specification* (March 2006)

IETF RFC 4514, *Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names* (June 2006)

IETF RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)* (September 2007)

IETF RFC 4862, *IPv6 Stateless Address Autoconfiguration* (September 2007)

IETF RFC 5116, *An Interface and Algorithms for Authenticated Encryption* (January 2008)

IETF RFC 5216, *The EAP-TLS Authentication Protocol* (March 2008)

IETF RFC 5234, *Augmented BNF for Syntax Specifications: ABNF* (January 2008)

IETF RFC 5480, *Elliptic Curve Cryptography Subject Public Key Information* (March 2009)

- IETF RFC 5722, *Handling of Overlapping IPv6 Fragments* (December 2009)
- IETF RFC 6066, *Transport Layer Security (TLS) Extensions: Extension Definitions* (January 2011)
- IETF RFC 6724, *Default Address Selection for Internet Protocol version 6 (IPv6)* (September 2012)
- IETF RFC 6818, *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* (January 2013)
- IETF RFC 6874, *Representing IPv6 Zone Identifiers in Address Literals and Uniform Resource Identifiers* (February 2013)
- IETF RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP* (June 2013)
- IETF RFC 7405, *Case-Sensitive String Support in ABNF* (December 2014)
- IETF RFC 7748, *Elliptic Curves for Security* (January 2016)
- IETF RFC 8032, *Edwards-Curve Digital Signature Algorithm (EdDSA)* (January 2017)
- IETF RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification* (July 2017)
- IETF RFC 8201, *Path MTU Discovery for IP version 6* (July 2017)
- IETF RFC 8398, *Internationalized Email Addresses in X.509 Certificates* (May 2018)
- IETF RFC 8399, *Internationalization Updates to RFC 5280* (May 2018)
- IETF RFC 8415, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)* (November 2018)
- IETF RFC 8439, *ChaCha20 and Poly1305 for IETF Protocols* (June 2018)
- IETF RFC 8446, *The Transport Layer Security (TLS) Protocol Version 1.3* (August 2018)
- IETF RFC 8504, *IPv6 Node Requirements* (January 2019)
- IETF RFC 8335, *PROBE: A Utility for Probing Interfaces* (February 2018)
- ANSI X9.62, *Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)* (2005)
- W3C EXI 1.0, *Efficient XML Interchange (EXI) Format 1.0, W3C Recommendation* (March 2011)
- IANA Service & Port Registry, *Service Name and Transport Protocol Port Number Registry* [viewed 2011-01-16], Available from: <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml>
- NIST FIPS PUB 180-4, *Secure Hash Standard (SHS)* (March 2012)
- NIST FIPS PUB 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions* (August 2015)
- ITU-T X.509, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks* (October 2019)
- IEEE 802.1X-2020, *IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control* (January, 2020)
- WPA3, *WPA3 Specification Version 3.0* (December 2020)

NIST Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC* (November 2007)

NIST Special Publication 800-56A, Revision 3, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography* (April 2018)

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1 access point AP

wireless communication device that allows the user to connect to other wireless or wired communication devices

3.2 authorization mode

authenticate and authorize the user account

Note 1 to entry: Authorization mode refers to *EIM* (3.17) and *PnC* (3.41).

3.3 automatic connection device pantograph ACDP

components supporting the automatic connection and disconnection process for conductive energy transfer between an EV and EVSE via pantograph

3.4 basic charging BC

charging based on PWM

Note 1 to entry: According to ISO/IEC 11889-1:2015, Annex A.

3.5 certificate

electronic document which uses a digital signature to bind a public key with an identity

Note 1 to entry: The ISO 15118 series describe several certificates covering different purposes [e.g. contract certificate including the *EMAID* (3.19) and *OEM* (3.36) provisioning certificates].

3.6 charging limit

set of physical constraints that is negotiated during a *service session* (3.50)

EXAMPLE Voltage, current, energy, power, etc.

3.7 charging session

collection of charging transactions at a charge point related only to the charging of an electric vehicle assigned to a specific customer in a specific timeframe with a unique identifier

Note 1 to entry: The charging session is a subset of the *service session* (3.50).

3.8

charging station operator

CSO

secondary actor responsible for the installation and operation of a charging infrastructure (including charging sites), and the management of electricity to provide the requested energy transfer services

Note 1 to entry: The term CSO for charge point operator is also used in other ISO 15118 documents. This term is not recommended for trademark reasons.

3.9

communication session

sequence of time where *EVCC* (3.21) and *SECC* (3.47) interactively exchange digital information in order to manage charging or discharging the EV battery

Note 1 to entry: A communication session can be paused and resumed later several times. The communication session encapsulates zero or more energy transfer periods.

3.10

communication setup timer

timer (3.61) monitoring the time between establishment of TLS connection and reception of *SessionSetupRes* by *EVCC* (3.21)

3.11

contract certificate

certificate (3.5) issued for the *EVCC* (3.21) by an *eMSP* (3.20) sub-CA (3.57), which is used in XML signatures on application layer so that the *SECC* (3.47) or secondary actor can verify the signature created by the *EVCC* with the contract certificate issued for that EV

Note 1 to entry: The secondary actor uses the *EMAID* (3.19), which is part of the contract certificate's subject field, to authorize the EV for charging based on the *eMSP*'s associated e-mobility contract.

3.12

CP state

control pilot state

state according to control pilot function defined in IEC 61851-1

3.13

credential

piece of information attesting an entity's identity

3.14

cross certificate

certificate (3.5) containing the public key of an existing certificate of a CA in one organization (called cross-certified CA) but signed by a root CA of another organization (called cross-certifying CA)

Note 1 to entry: With cross-certification, an end-entity, who only trusts a cross-certifying root CA, can validate a certificate chain issued by the root CA of another organization through a cross certificate appended to the chain.

3.15

distinguished encoding rules

DER

method for encoding a data object, such as an ITU-T X.509 *certificate* (3.5), to be digitally signed or to have its signature verified

3.16

dynamic control mode

control mode for the communication

Note 1 to entry: Further Information can be found in ISO 15118-1.

Note 2 to entry: The *SECC* (3.47) controls the power flow and gives the *EVCC* (3.21) set points it should follow.

3.17

external identification means

EIM

authorization means that are handled outside of this document

3.18

elliptic curve cryptography

ECC

mechanism for implementing public-key cryptography based on the discrete logarithms by algebraic structure of elliptic curves

3.19

eMobility account identifier

EMAID

contract identification for the contract that is issued by the *eMSP* (3.20) and used by the *SECC* (3.47) or secondary actor to enable energy transfer and related services (including billing)

Note 1 to entry: The term contract ID is not used anymore in this document. It has been replaced by the term EMAID. The definition is still there for compatibility with ISO 15118-1.

3.20

eMobility service provider

eMSP

entity with which the customer has a contract for all services related to the EV energy transfer

Note 1 to entry: Typically, the eMSP will include some of the other actors, like spot operator or EP, and has a close relationship with the distribution system operator and meter (3.33) operator. An *OEM* (3.36) or utility could also fulfil such a role.

Note 2 to entry: eMSPs validate *EMAIDs* (3.19) from their customers, which were received either from the EMOCH, other eMSPs or spot operators the customer is in relation with.

Note 3 to entry: eMSPs issue EMAIDs to their customers.

3.21

electric vehicle communication controller

EVCC

embedded system, within the vehicle, that implements the communication between the vehicle and the *SECC* (3.47) in order to support specific functions

Note 1 to entry: Such specific functions could be, e.g. controlling input and output channels, encryption, or data transfer between vehicle and SECC.

3.22

EVPowerProfile

scheme which contains the power limits for charging or discharging the battery during an energy transfer period

Note 1 to entry: Refer to definition of "energy transfer schedule" in ISO 15118-1.

Note 2 to entry: In *dynamic control mode* (3.16) it describes a simulation from the EVs perspective on the fastest charging profile in order to reach the *EVMaximumEnergyRequest* under the constraint of the minimum of the *EVSEMaximumChargePower* and *EVMaximumChargePower*.

EXAMPLE The schedule is calculated based on target setting, sales tariff table and grid schedule information, respecting the corresponding current limitations, i.e. using the lowest current value.

3.23

electric vehicle supply equipment ID

EVSEID

unique identification of the EVSE

3.24

electric vehicle supply equipment

EVSE

<conductive power transfer> conductors, including the phase(s), neutral and protective earth conductors, the EV couplers, attached plugs, and all other accessories, devices, power outlets or apparatuses installed specifically for the purpose of delivering energy from the premises wiring to the EV and allowing communication between them as necessary

3.25

electric vehicle supply equipment

EVSE

<wireless power transfer> off-board equipment comprising the SECC (3.47) and one or multiple supply devices working under the control of the same SECC

3.26

global address

IP address (3.28) with unlimited scope

3.27

high level communication charging

HLC-C

energy transfer phase during a *service session* (3.50)

3.28

IP address

address

IP-layer identifier for an interface or a set of interfaces

3.29

link-local address

IP address (3.28) with link-only scope that can be used to reach neighboring interfaces attached to the same link

3.30

maximum transfer unit

MTU

maximum size (in bytes) of the largest protocol data unit that the data link layer that can pass onwards

3.31

message set

set of *V2G messages* (3.66) and parameters for the *EVCC* (3.21) or *SECC* (3.47) covering one or multiple use case elements

3.32

message timer

timer (3.61) monitoring the exchange of a request-response-pair

3.33

meter

analogic device able to measure the amount of energy used and to monitor it

3.34

multiplexed communication

MC

exchange of multiple messages with different payload types over the *V2GTP* (3.68) connection between the *EVCC* (3.21) and *SECC* (3.47)

3.35

node

device that implements IPv6

3.36

original equipment manufacturer

OEM

producer who manufactures products or components that are purchased by a company and retailed under that purchasing company's brand name

Note 1 to entry: OEM refers to the company that originally manufactured the product.

Note 2 to entry: When referring to automotive parts, OEM designates a replacement part made by the manufacturer of the original part.

3.37

OEM provisioning certificate

certificate (3.5) issued to the *EVCC* (3.21) by the *OEM* (3.36) to enable the provisioning of a *contract certificate* (3.11)

Note 1 to entry: It is securely requested and received from a secondary actor to uniquely identify the EVCC.

3.38

PE certificate

leaf *certificate* (3.5) issued in *PE* (3.42) to a *private SECC* (3.43) by a PE private root CA or optionally by a PE sub CA, which is used in TLS so that the *EVCC* (3.21) can verify the authenticity of the private SECC

3.39

PE EVSE

EVSE that is operating in a *private environment* (3.42) and is containing or being controlled by a *private SECC* (3.43)

3.40

performance time

non-functional timing requirement defining the time a *V2G entity* (3.65) should not exceed when executing or processing certain functionality

Note 1 to entry: This is a fixed time value.

3.41

park and charge

PnC

authorization mechanism using *certificates* (3.5) stored in the EV which does not require any user interaction

3.42

private environment

PE

area of private responsibility with physical access limited to a small number of vehicles

3.43

private SECC

SECC (3.47) operating in a *private environment* (3.42) that uses a *PE certificate* (3.38)

Note 1 to entry: *PE* (3.42) usually implies lower security. In most cases SECC requirements will also apply to a private SECC. In some specific cases, the SECC and private SECC requirements can be distinct. Those cases and requirements will be called out as such.

3.44

public SECC

SECC (3.47) operating in a public environment that uses a *PE certificate* (3.38)

3.45

request-response message pair

request message and the corresponding response message

3.46

request-response message sequence

predefined sequence of *request-response message pairs* (3.45)

3.47

supply equipment communication controller

SECC

entity which implements the communication to one or multiple *EVCCs* (3.21) and which may be able to interact with secondary actors

Note 1 to entry: Functions of a supply equipment communication controller may control input and output channels, data encryption, or data transfer between vehicle and SECC.

3.48

SECC certificate

leaf *certificate* (3.5) issued to an *SECC* (3.47) by a *CSO* (3.8) sub-CA2, which is used in TLS so that the *EVCC* (3.21) can verify the authenticity of the SECC

3.49

sequence timer

timer (3.61) monitoring a *request-response message sequence* (3.46)

3.50

service session

collection of services around a charge point mainly related to the charging of an EV assigned to a specific customer in a specific timeframe with a unique identifier

Note 1 to entry: *Charging session* (3.7) and WPT session are some kinds of service sessions.

3.51

scheduled control mode

control mode for the communication

Note 1 to entry: Further Information can be found in ISO 15118-1.

Note 2 to entry: The *EVCC* (3.21) and *SECC* (3.47) negotiate a power profile for charging or discharging purposes.

3.52

schedule renegotiation

messaging for updating the agreement on the energy transfer schedule between the *EVCC* (3.21) and *SECC* (3.47) during a *V2G communication session* (3.64) by retransmitting the parameters schedule and *EVPowerProfile* (3.22)

3.53

station

STA

logical entity that is a singly addressable instance of a medium access control and physical layer interface to the wireless medium which does not act as an *access point* (3.1)

3.54

SDP client

V2G entity (3.65) that uses the *SDP server* (3.55) to get configuration information about the *SECC* (3.47) to be able to access the SECC

3.55

SDP server

V2G entity (3.65) providing configuration information for accessing the *SECC* (3.47)

3.56

smart meter

device that is able to measure and monitor the energy used or generated

Note 1 to entry: In this case during EV *charging session* (3.7).

Note 2 to entry: The values for active/reactive energy, active/reactive power, current, power factor, based on timing slot can be recorded. The values are monitored remotely, so they can be programmed to manage the power (for example, reducing or modulating it). Furthermore, the values can share the information with DSO and other devices based on PLC communication.

3.57 **sub-CA**

subordinate certificate authority which issues, e.g. *SECC certificates* (3.48) and/or *contract certificates* (3.11) on behalf of a root CA such as *V2G root CA* (3.70) or e-mobility service provider root CA (the latter only for contract certificates)

Note 1 to entry: The ability of issuing the certificates are delegated from a root CA and a root CA can revoke the sub-CA at any time.

3.58 **sub-CA certificate** *certificate* (3.5) issued to sub-CA (3.57)

3.59 **TCP_DATA** socket interface for data transfer based on TCP connection

3.60 **timeout** timing requirement defining the time a *V2G entity* (3.65) monitors the communication system for a certain event to occur

Note 1 to entry: If the specified time is exceeded, the respective *V2G entity* (3.65) initiates the related error handling. This is a fixed-time value.

3.61 **timer** device or piece of software used in an implementation for measuring time

Note 1 to entry: Depending on the specific use case a timer is used to trigger certain system events.

3.62 **vehicle certificate** *leaf certificate* (3.5) issued to an *EVCC* (3.21) by an *OEM* (3.36) or *V2G* (3.63), which is used in TLS so that the *SECC* (3.47) can verify the authenticity of the *EVCC*

Note 1 to entry: This certificate is also used for binding between different TLS sessions that belong to the same V2G session by SECC.

3.63 **vehicle to grid** **V2G** plug-in electric vehicle interaction with the electric grid, including charging as well as discharging and bi-directional communication interface

Note 1 to entry: The first part of this definition is excerpted from the scope of the V2G domain expert working group, SGIP, NIST.

3.64 **V2G communication session** association of two specific V2G entities for exchanging *V2G messages* (3.66)

3.65 **V2G entity**

primary actor participating in the V2G communication

Note 1 to entry: Primary actors can be the *EVCC* (3.21) or *SECC* (3.47).

3.66

V2G message

message exchanged on application layer

Note 1 to entry: Refer to Clause 8.

3.67

V2G setup

setup phase for V2G messaging

3.68

V2G transfer protocol

V2GTP

communication protocol to transfer *V2G messages* (3.66) between two V2GTP entities

3.69

V2GTP entity

V2G entity (3.65) supporting the *V2G transfer protocol* (3.68)

3.70

V2G root CA

certificate authority (CA) which issues sub-CA (3.57) certificates to sub-CAs

Note 1 to entry: Those sub-CAs are then delegated to issue either certificates to a second sub-CA (sub-CA2) or to directly issue leaf certificates, such as *contract certificate* (3.11) or *SECC certificates* (3.48).

3.71

V2G root CA certificate

certificate issued to *V2G root CA* (3.70)

4 Abbreviated terms

The abbreviations given in ISO 15118-1 and the following apply.

AC	alternating current
ACDP	automatic connection device pantograph
CPDA	DC_ChargeParameterDiscovery
AKI	authority key identifier
AP	access point
APOS	ACDP_VehiclePositioning
ASUP	AuthorizationSetup
AUTH	authorization
BEV	battery electric vehicle
BPT	bidirectional power transfer
CA	certificate authority

CC	CableCheck
CINS	CertificateInstallation
CONA	ACDP_Connect
CPM4PE	certificate provisioning mode for private environment
CPS	certificate provisioning service
CRL	certificate revocation list
CSO	charging station operator
DC	direct current
DCCL	DC_ChargeLoop
DH	Diffie Hellman
DER	distinguished encoding rules
DISA	DisconnetACDP
EAP	extensible authentication protocol
ECDSA	elliptic curve digital signature algorithm
EdDSA	Edwards-curve digital signature algorithm
EMA	e-mobility account
EMAID	e-mobility account identifier
EMOCH	e-mobility operator clearing house
eMSP	eMobility service provider
ESDW	emergency shut down
EV	electric vehicle
EVCC	electric vehicle communication controller
EVRESS	electric vehicle rechargeable energy storage system
EVSE	electric vehicle supply equipment
EVSEID	electric vehicle supply equipment identification
EXI	efficient XML interchange
HLC-C	high level communication charging
IV	initialization vector
MCON	MeteringConfirmation
NACK	negative acknowledgement

OCSP	online certificate status protocol
OEM	original equipment manufacturer
OID	object identifier
PC	PreCharge
PD(Start)	PowerDelivery(Start)
PD(Stop)	PowerDelivery(Stop)
PDU	protocol data unit
PE	private environment
PHEV	plug-in hybrid electric vehicle
PKI	public key infrastructure
PLC	power line communication
PMF	protected management frames
PnC	park and charge
PPD	pairing and positioning device
RFC	request for comments(IETF)
SA	secondary actor
SAID	secondary actor ID
SAP	SupportedAppProtocol
SDE	ServiceDetails
SDI	ServiceDiscovery
SDP	SECC discovery protocol
SDU	service data unit
SE	ScheduleExchange
SECC	supply equipment communication controller
SKI	subject key identifier
SOC	state of charge
SSEL	ServiceSelection
SSU	SessionSetup
SSP	SessionStop
SYSS	ACDP_SystemStatus

TCP transmission control protocol

UDP user datagram protocol

VAS value added service

V2G vehicle to grid

NOTE V2G as is used in this document only means the communication between EVCC and SECC.

V2G CI vehicle-to-grid communication interface

V2GTP V2G transfer protocol

WMI world manufacturer identifier

WPT wireless power transfer

XML extensible markup language

5 Conventions

5.1 Definition of OSI based services

This document is based on the conventions defined in the OSI service conventions (refer to ISO/IEC 10731) as they apply for the individual layers specified in this document.

This document describes requirements applicable to layer 3 – 7 according to the OSI layered architecture.

5.2 Requirement structure

This document uses the requirement structure defined here. A unique number identifies each individual requirement defined in this document. Systematic and ordered requirement structure enables readers to find the target requirement number easily.

The following format is applied for new defined and updated requirements:

[V2G20-xxxx] requirement text, where:

- ‘V2G20’ represents this document;
- ‘xxxx’ represents the unique requirement number consisting of four digits starting from 1 000;
- ‘requirement text’ defines the actual text of the requirement.

EXAMPLE **[V2G20-1000]** This is an example requirement introduced in this document.

The format below is applied to the handed over requirements from ISO 15118-2:

[V2G20-yyy] requirement text, where:

- ‘V2G20’ represents this document;
- ‘yyy’ represents the unique requirement number same as already defined in ISO 15118-2;
- ‘requirement text’ is the same text as defined in first edition.

EXAMPLE **[V2G20-000]** This is an example requirement originally defined in ISO 15118-2.

5.3 Usage of references

[V2G20-1230] All published updates and error corrections (errata) shall be applied to the referred documents.

NOTE This does not include updated RFC or other requirement numbers not referenced in Clause 2 or Bibliography. This additionally does not include requirements published after publication of this document.

EXAMPLE If an errata to IETF RFC 8446 for TLS 1.3 is published 2 months after publication of this document and simply provides correction to an existing spec without which TLS 1.3 could not be implemented, that errata can be considered during implementation of this document. But if an IETF RFC is published 2 months after publication of this document and updates TLS 1.3 to TLS 1.4 due to some major issues in the protocol, this IETF RFC cannot be considered for implementation of this document as it can result in unforeseen issues.

5.4 Notation used for XML schema diagrams

This document makes use of XML as a description format for V2G messages. For details with regards to the XML schema diagram notation used in this document refer to Reference [95].

Allowing for an easy way to distinguish the types used for the XML schema definitions in this document, the following naming conventions apply:

- complex type use capitalized first letters,
- simple types use non capitalized first letters.

6 Document overview

Figure 2 describes the organization of the different documents in the ISO 15118 series and the usage of the subclauses, according to the OSI layered architecture.

As indicated by the bold framed shapes, this document defines requirements applicable to layers 3 – 7 according to the OSI layered architecture. Layer 1 and layer 2 requirements including the V2G standardized service primitive interface are specified in ISO 15118-3 and ISO 15118-8.

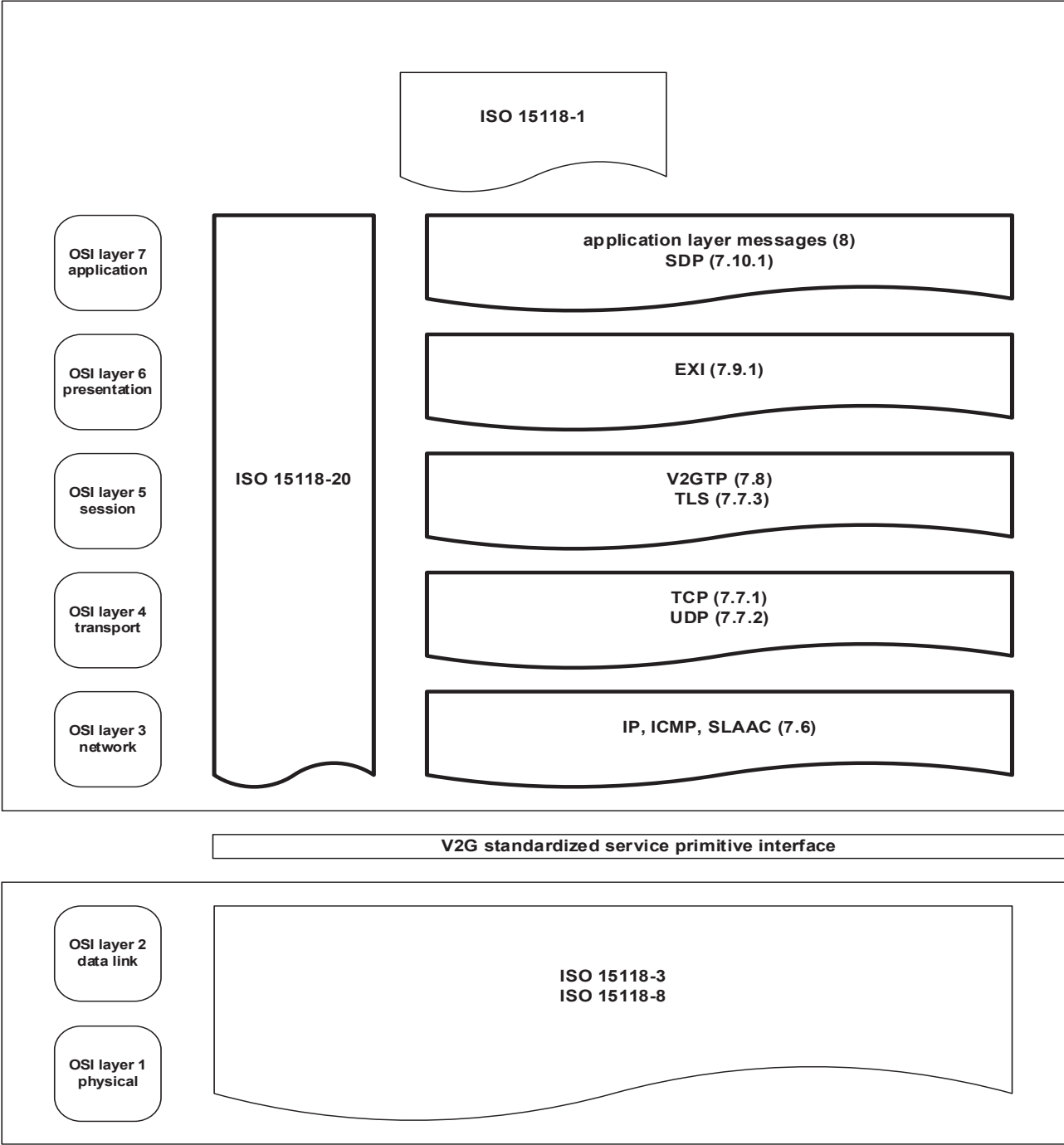


Figure 2 — Vehicle to grid communication document overview

7 Basic requirements for V2G communication

7.1 General information

This document describes the realization of the V2G use case elements defined in ISO 15118-1.

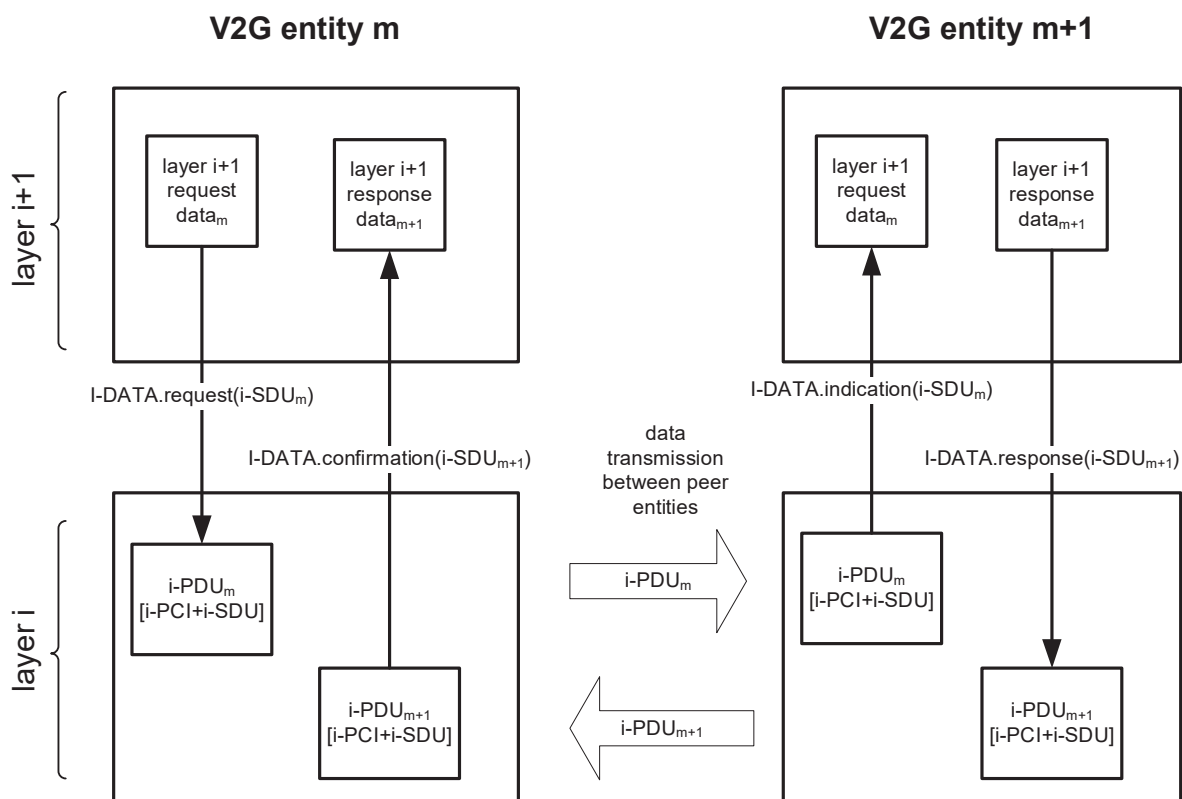
7.2 Service primitive concept of OSI layered architecture

7.2.1 Overview

This subclause explains how the OSI layered architecture is applied for the purpose of this document. It is intended to provide simple means for describing the interfaces between the individual communication protocol layers required by this document and furthermore allows for defining timing requirements more precisely.

Services are specified by describing the service primitives and parameters that characterize a service. This is an abstract definition of services and does not force a particular implementation.

Figure 3 depicts a simplified view of OSI layer interaction sufficient to understand the OSI layered architecture principles for the context of this document.



Key

PDU_x: protocol data unit of network entity x

PCI: protocol control information

SDU_x: service data unit of network entity x

Figure 3 — OSI layered architecture principles

When a layer i+1 instance of V2G entity m exchanges data with a layer i+1 instance of V2G entity m+1 each instance uses services of an instance of layer i. A service is defined as a set of service primitives.

7.2.2 Syntax of service primitives

Service primitives are described with the following syntax:

- [Initial of layer]-[NAME].[primitive type](parameter list);
 - a) whereas [initial of layer] is one out of the following seven:

- physical, data link, network, transport, session, presentation, application;

b) whereas [NAME] is the name of the primitive;

EXAMPLE Typical examples for [Name] are CONNECT, DISCONNECT, DATA; other names are used in this document and ISO 15118-3.

c) whereas [primitive type] is one out of the following four:

- request, indication, response, confirmation;

d) whereas (parameter list) includes a list of parameters separated by comma the user of the service is supposed to provide when using the respective service primitive; optional parameters are marked with brackets "[..]".

NOTE In this document, the primitive type ".indication" always indicates an event asynchronously to the upper layer.

7.3 Security concept

7.3.1 General

This subclauses provide specific and separate requirements for the private SECC and the SECC. Thus, unless otherwise specified, private SECC and SECC are not considered interchangeable.

In ISO 15118-2, transport layer security (TLS) was only required for PnC or VAS. In this document, TLS is always mandatory. For backward compatibility, connection setup processes will accept both ISO 15118-2 handling and the handling defined in this document. This means the connection setup processes will not change.

If an application still requires optional TLS, ISO 15118-2 shall be used. Refer to 7.7.3.10 for further details.

Figure 4 depicts the principal approach for various cases from a security point of view, showing the necessary security services applied as well as an abstract view on the different data flows necessary for the operation.

The data flow/sequence diagrams can be found in 8.6.6. In Figure 4, only the security relevant information is highlighted.

The security concept provides a basic transport based protection mechanism. For all scenarios described in this document, the usage of TLS for the transport communication between the EVCC and SECC is mandatory. In case data should be protected to or from a secondary actor or if the protection should last longer than the existence of the TLS channel, specific messages could be protected on application layer (XML-based signatures).

Figure 4 shows an example sequence for a PnC scenario. As described in Figure 4, all TCP/IP based communication is protected using a mutually authenticated TLS channel between the two peers.

Some of the information provided by the EVCC may need to be sent to the SA for further processing. The EVCC calculates a power profile (refer to 8.3.4.3.8.2) and sends it to the SECC. The SECC may send it to SA systems like energy management system or demand clearing house. Further process is similar to the semi-online case with the exception that the final charging data can be directly submitted to the SA. It is assumed that the SECC will also use a secure transport connection to the SA.

NOTE The communication between SECC and SA in Figure 4 is shown for informational purpose only and not intended to specify a particular message sequence.

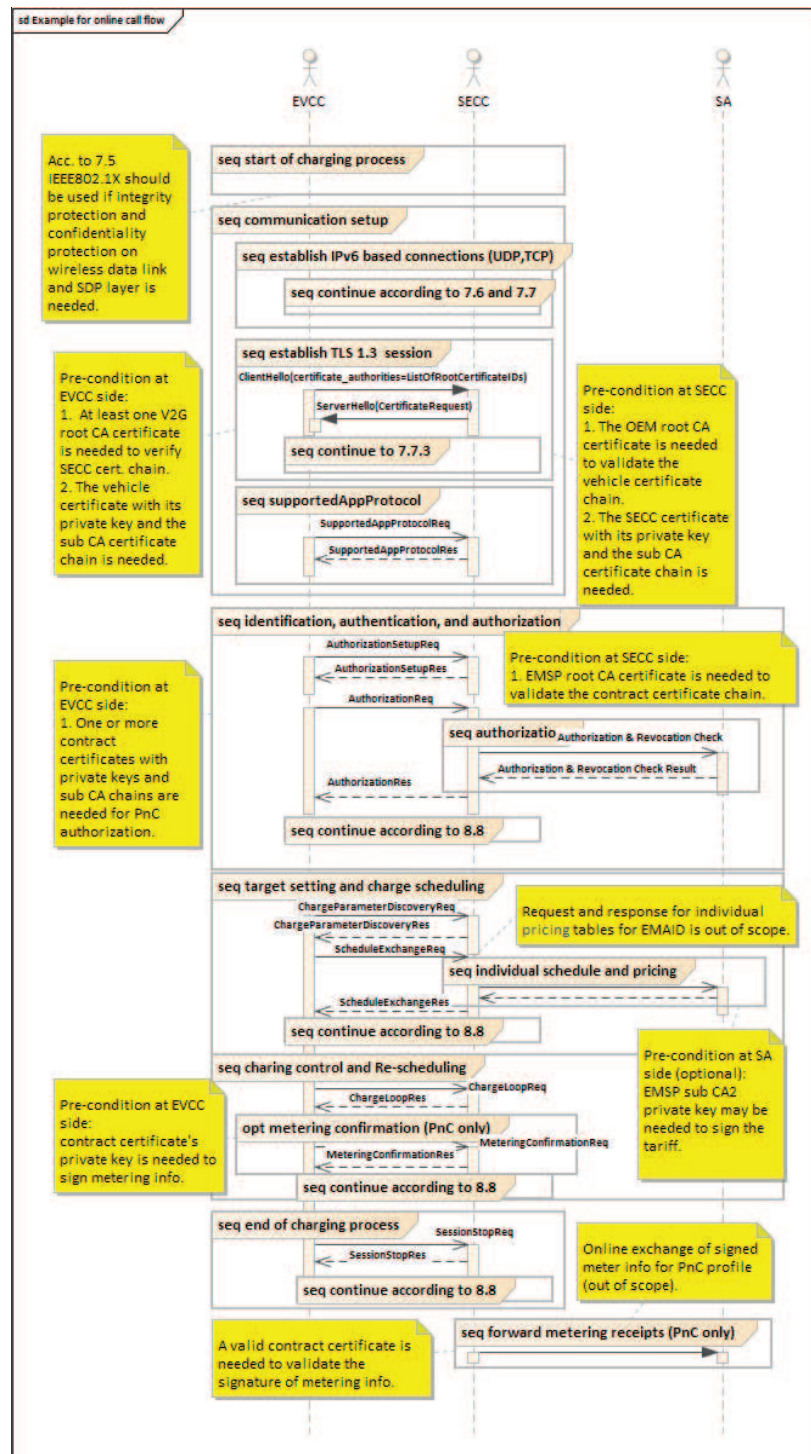


Figure 4 — Example for call flows

There are further use cases where security mechanisms are needed on application layer. These are the initial enrollment/installation of contract certificates and keys as well as the update of the contract certificates and keys. In this case vehicle specific OEM keys are used. Those mechanisms are described in 7.9.2.5. An overview on all needed certificates can be found in Annex B.

While storing any data related to certificates/messages provided by the EVCC, the EVSE and the SAs (including CSO/eMSP/OEM/etc.) should be cognizant of the local/state/national/international privacy rules, regulations and requirements. These rules/regulations/requirements are not in the scope of this document but should be taken into account when designing and implementing the solution.

7.3.2 Certificate and key management

The call flows shown in 7.3.1 require the existence of multiple certificates to be applied for the different security layers. There are SECC certificates used in the TLS layer for the EVCC to authenticate SECC. There are contract certificates used at the application layer to authenticate against an SECC and/or SA. There are V2G root CA certificates and possibly sub-CA certificates which certify SECC certificates and contract certificates.

Separate from above certificates, there are OEM root CA certificates and vehicle certificates used in the TLS layer for the SECC to authenticate the EVCC. OEM provisioning certificates that stem from OEM root CA certificates may be used for installing and updating contract certificates.

Requirements for various certificates can be found in 7.3.2.1. For an overview of all possible certificate profiles, see Annex B. For examples of the certificate structures, see Annex H.

[V2G20-1231] Each V2G entity shall use X.509v3 certificates.

Table 1 shows what fields an X.509v3-certificate consists of:

Table 1 — Basic certificate fields

Certificate field	Description
Version	Version of certificate (for 15118 it shall be v3 = 0x2)
Serial number	Unique number of certificate (within the domain of the issuer)
Signature algorithm	Used signature algorithm
Issuer	Entity, who has issued and signed the certificate
Validity period	Time period, in which the certificate is valid
Subject	Entity, to which the certificate is issued
Public key	Public key corresponding to a private key
Issuer UID	Optional issuer unique identifier
Subject UID	Optional subject unique identifier
Extensions	Additional attributes associated with entities or public keys or used to manage relationships between CAs
Signature	Signature of the certificate generated by the issuer

NOTE 1 For those not familiar with the various fields, refer to IETF RFC 5280 and ITU-T X.509.

NOTE 2 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.

Depending on the use case, additional information may be included using so called certificate extensions. Table 2 summarizes common certificate extensions.

Table 2 — Certificate extension examples

Certificate extensions	Description
Key usage	Usage of the corresponding private key (e.g. Digital Signature, non-repudiation, key encipherment, ...)

Extended Key Usage	<p>Further specification of key usage using OIDs, e.g.:</p> <ul style="list-style-type: none"> – server authentication (1.3.6.1.5.5.7.3.1); – client authentication (1.3.6.1.5.5.7.3.2). <p>NOTE Sometimes the following values are encoded here:</p> <ul style="list-style-type: none"> – Netscape SGC (1.3.6.1.4.1.311.10.3.3) – Microsoft SGC (2.16.840.1.113730.4.1) <p>SGC stands for server gated crypto and indicates that the server can also use strong cryptography for the connection with the client's browser. This extension was used at the time of strong crypto export control to enable financial web site to provide appropriate protection of the data transfer.</p>
CRL distribution point	Location to retrieve certificate revocation lists
OCSP	Location to retrieve OCSP. Refer to IETF RFC 6960 as updated by IETF RFC 8954 for details.
Authority information	Additional authorization information
Subject alternative name	Alternative names of the entity
Basic constraint = CA	True if the certificate is a root certificate or a sub-CA certificate.
subjectAltPublicKeyInfo	Alternative/secondary certificate key data. This contains the alternative key algorithm and the alternative key generated using the said algorithm. Refer to ITU-T X.509 for further details.

NOTE 3 For those not familiar with OIDs, e.g. 1.3.6.1.5.5.7.3.1, refer to the Object Identifier (OID) Repository.

[V2G20-2673] Each V2G entity shall support Hash-operation SHA-512 (signature process) according to NIST FIPS PUB 180-4 (for ISO 15118-1, use case element ID: F1).

[V2G20-2318] Each V2G entity shall support SHAKE256 according to NIST FIPS PUB 202 (for ISO 15118-1, use case element ID: F1).

[V2G20-2674] Each V2G entity shall support signature operations using ECC based elliptic curve (secp521r1[SECG notation]) with signature algorithm ECDSA (for ISO 15118-1, use case element ID: F1).

[V2G20-2319] Each V2G entity shall additionally support signature operations with ECC algorithm Ed448 (for ISO 15118-1, use case element ID: F1), i.e. signature algorithm EdDSA using elliptic curve Curve448 (or Curve448-Goldilocks) in Edwards form, see IETF RFC 7748 and IETF RFC 8032.

NOTE 4 In case V2G entity chooses to use Curve448-based signature algorithm, it also uses ECC-based DH algorithm X448 defined for this curve (see IETF RFC 7405), in addition to the algorithms specified by NIST Special Publication 800-56A. See also [V2G20-2710] and [V2G20-2711].

[V2G20-2320] Multiple algorithms are integrated to allow for cryptographic agility. Each V2G entity shall implement a secure configurable mechanism to securely switch usage of (elliptic curve) EC from that defined in [V2G20-2674] to the one defined by [V2G20-2319] and prevent the usage of a particular algorithm, e.g. in case a security flaw was found in the preferred ECC algorithm.

NOTE 5 The design and implementation of this configuration mechanism is not in the scope of this document.

NOTE 6 secp521r1 is a very common ECC algorithm supported by NIST. Curve Ed448 is not as widely used at the time of the publication of this document. Although there are quite a few implementations supporting curve Ed448, secp521r1 is used as the main curve due to its ubiquity. In case flaw(s) are found in the secp521r1, availability of the alternative curves allows implementers to quickly switch to a parallel algorithm without the need for implementation and validation of a new cryptographic algorithm. This ensures that the implementers/operators can quickly respond to any reported vulnerabilities in secp521r1.

[V2G20-2321] As long as no issues or flaws are identified in the (elliptic curve) EC as specified by [V2G20-2674], the (elliptic curve) EC as specified by [V2G20-2674] shall be considered the preferred ECC algorithm. The mechanism defined by [V2G20-2320] shall only be updated to usage of (elliptic curve) EC as defined by [V2G20-2319] when there are issues/flaws identified with the (elliptic curve) EC as specified by [V2G20-2674].

NOTE 7 By default the mechanism defined by [V2G20-2320] can be set to use (elliptic curve) EC as specified by [V2G20-2674].

[V2G20-2675] Each V2G entity shall support a key length of 521 bits for ECC based asymmetric cryptography.

NOTE 8 Additionally, key length of 448 bits is used with certain curves in the application of this document. If a V2G entity can manage and utilize 521 bit keys, it can be capable of managing and utilizing 448 bit keys as well.

[V2G20-2322] Each certificate shall meet all requirements as specified for that certificate in this subclause (and any of its subclauses), 7.3.3 (and any of its subclauses) and in Annex B.

NOTE 9 Annex B provides the certificate profiles.

[V2G20-926] The certificate extensions mentioned in Annex B shall be supported.

NOTE 10 Where necessary, deviations have been specified.

[V2G20-2323] Certificates used in this document shall not contain any extensions other than those specified in Annex B.

NOTE 11 If an extension is mentioned as allowed for a certificate profile in Annex B, regardless whether it is marked as mandatory or optional, a certificate generated to meet that certificate profile is permitted to utilize that extension. If the extension is not mentioned as allowed in the corresponding certificate profile, that extension cannot be present in the corresponding certificate. For example, 'CertificatePolicies' extension is marked as optional in most profiles. That means whether the 'CertificatePolicies' extension is included is up to the certificate issuer's and certificate requester's discretion. On the other hand, since the 'subjectDirectoryAttributes' extension is not specified as a mandatory or optional extension by Annex B, the 'subjectDirectoryAttributes' extension cannot be included in any certificate used in this document.

NOTE 12 This ensures that incompatible extensions do not result in unforeseen issues or result in interoperability concerns.

[V2G20-1234] Each certificate in a certificate chain shall be DER encoded and the size of each certificate in DER encoded form shall be limited to a maximum of 1 600 bytes. Refer to ITU-T X.509 for details of DER encoding.

NOTE 13 A certificate chain is made up of multiple certificates. [V2G20-1234] applies to each certificate in the certificate chain, not the entire certificate chain itself. If a certificate chain is made up of four certificates, that chain will be a maximum of 6 400 bytes in DER format.

NOTE 14 As mentioned in Annex B, there are many mandatory and optional parameters in a certificate. Some parameters have well defined fixed lengths while others are variable length parameters. The certificate issuer can experiment with different optional parameters, different parameter data for variable length parameters, etc. to stay within the bounds of [V2G20-1234]. For example, if the OCSP responder address is too long, the certificate issuer can use methodologies to shorten the address to keep the certificate length within the bounds of [V2G20-1234].

[V2G20-1004] Certificates shall be issued and signed by the CA within the validity of its own certificate.

[V2G20-911] If only one sub-CA layer is used, i.e. a sub-CA signed by a root CA directly signs leaf certificates, the profile of sub-CA2 shall apply for that sub-CA.

[V2G20-1003] All certificate chains (except where a cross certificate is used) shall have a maximum length of 3.

NOTE 15 The certificate chain includes the leaf certificate. The certificate chain does not include the root certificate.

NOTE 16 This means, at most two sub-CA levels can be used.

[V2G20-1005] All certificate chains, including a cross certificate, shall have a maximum length of 4.

NOTE 17 The certificate chain includes the leaf certificate and the cross certificate. The certificate chain does not include the root certificate.

NOTE 18 A cross certificate adds one more level.

[V2G20-1002] When cross-certification is used, the certificate chain sent shall include the cross-certificate.

NOTE 19 The profile of a cross certificate differs from that of other CA certificates by the validity period and the use of Subject Information Access extension. See Annex B for further details.

[V2G20-1853] A cross-certificate shall not be valid beyond the validity period of the cross-certified CA's certificate and cross-certifying CA's certificate.

[V2G20-1001] All certificate validations shall be carried out in conformance with IETF RFC 5280 and ITU-T X.509. During certificate validation, each certificate shall be checked for conformance with the appropriate profile in Annex B. All requirements from Annex B shall be met for the appropriate certificate profile. The EVCC and the SECC shall cache certificate validation results during one service session.

NOTE 20 The certificate validation includes checking the following.

- a) The content of a 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.
- b) The signature up to the trust anchor level is not compromised (none of the certificates have been revoked). Certificate revocation is checked via the OCSP response (or CRL, if allowed for that particular certificate) as detailed in 7.7.3.1 and 7.7.3.3.
- c) The validity period of each certificate in the chain up to the trust anchor has not yet elapsed.
- d) Each certificate in the certificate chain matches the appropriate certificate profile as defined in Annex B. This includes checking the following:
 - the key length of each certificate in the certificate chain matches the key length specified by that certificate's profile in Annex B;
 - every critical KeyUsage attribute is set to the appropriate value (i.e. 0 or 1) as defined for that certificate's profile in Annex B;
 - every mandatory parameter, as defined for that certificate's profile in Annex B, exists;
 - all BasicConstraints attributes are set as defined for that certificate's profile in Annex B;
 - DomainComponent value matches the definition of that certificate's profile in Annex B;
 - the subjectID of the leaf certificate is acceptable [e.g. if the CN (common name) of the certificate is accepted by the V2G entity];
 - the subjectID of the leaf certificate is acceptable [e.g. if the CN (common name) of the certificate is accepted by the V2G entity].
- e) All critical parameters are processed.
- f) All non-critical parameters that are recognized by the relying party are processed.

NOTE 21 A V2G entity can use the services of a secondary actor to carry out one or more of these validation steps. For example, the SECC can use the service of a secondary actor to receive revocation information for each certificate in the certificate chain the EVCC provided.

NOTE 22 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.

[V2G20-2324] When the configurable mechanism as defined by [V2G20-2320] indicates that the curve as defined by [V2G20-2319] needs to be used, certificates and certificate profiles as defined in Table B.4, Table B.6, Table B.8, Table B.10, Table B.12, Table B.14, Table B.16 and Table B.18 for that particular certificate type shall be used during certificate validation (as defined by [V2G20-1001]).

[V2G20-2325] When the configurable mechanism as defined by [V2G20-2320] indicates that the curve as defined by [V2G20-2674] needs to be used, certificates and certificate profiles as defined in Table B.3, Table B.5, Table B.7, Table B.9, Table B.11, Table B.13, Table B.15 and Table B.17 for that particular certificate type shall be used during certificate validation (as defined by [V2G20-1001]).

7.3.2.1 Certificate structure

This document does not provide any mandatory PKI for implementations. It, however, defines a minimum required certificate structure that should be followed ensuring that the system as a whole is functioning. The details of the PKI, though, are left to the industry and implementers to define. For examples of the possible certificate structures/PKI, see H.1.6.

[V2G20-2581] When using the curve as defined by [V2G20-2674], each certificate used in this document shall comply to the appropriate profile as specified in Annex B, Table B.3, Table B.5, Table B.7, Table B.9, Table B.11, Table B.13, Table B.15 and Table B.17. When using the curve as defined by [V2G20-2319], each certificate used in this document shall comply to the appropriate profile as specified in Annex B, Table B.4, Table B.6, Table B.8, Table B.10, Table B.12, Table B.14, Table B.16 and Table B.18.

NOTE 1 Although Annex B defines certificate profiles with the two different curves, as defined by [V2G20-2674] and [V2G20-2319], it is not mandatory for a V2G entity to have certificates with both curves available at the same time. It is up to the V2G entity's discretion whether to store certificate chains with both curves at the same time or just the ones as required to be used per the configurable mechanism as defined by [V2G20-2320]. If the V2G entity chooses to store certificate chains based on just one curve, the V2G entity will need a capability to replace those certificate chains with different ones when the configurable mechanism as defined by [V2G20-2320] is updated to use the secondary curve.

[V2G20-2326] An SECC certificate shall be generated using a certificate chain that uses a V2G root CA certificate as the trust anchor. Refer to Figure 5 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of a certificate structure. Refer to Annex B for details of the certificate profile.

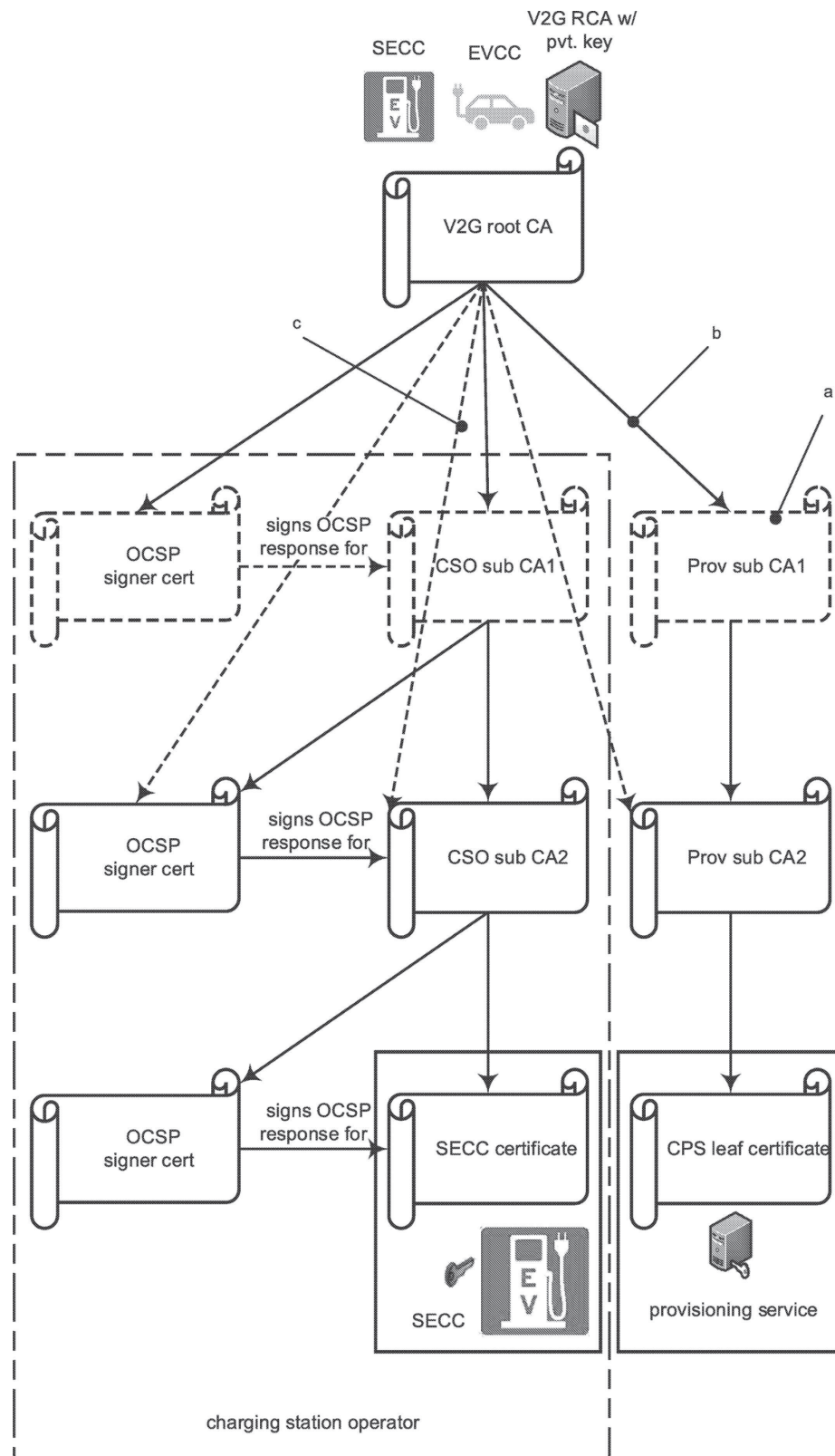
NOTE 2 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the CSO's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use as the trust anchor for the SECC certificate in their SECCs.

[V2G20-2327] An OCSP signer certificate used to sign the OCSP response for SECC certificate status shall be generated using a certificate chain that uses a V2G root CA certificate as the trust anchor. Refer to Figure 5 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of a 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, it is up to the CSO's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use as the trust anchor for the OCSP signer certificate that signs the OCSP response for their SECC certificates.

[V2G20-2328] A CPS leaf certificate shall be generated using a certificate chain that uses a V2G root CA certificate as the trust anchor. Refer to Figure 5 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of a certificate structure. Refer to Annex B for details of the certificate profile.

NOTE 4 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the CPS' discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use as the trust anchor for their CPS leaf certificate.



Key

- ^a Optional certificate – If the sub-CA1 is not present, the sub-CA2 is signed by the V2G root CA.
- ^b Direct certification – The use of sub-CA1 is optional.
- ^c Optional direct certification – If the sub-CA1 is present, it signs the sub-CA2 certificates.

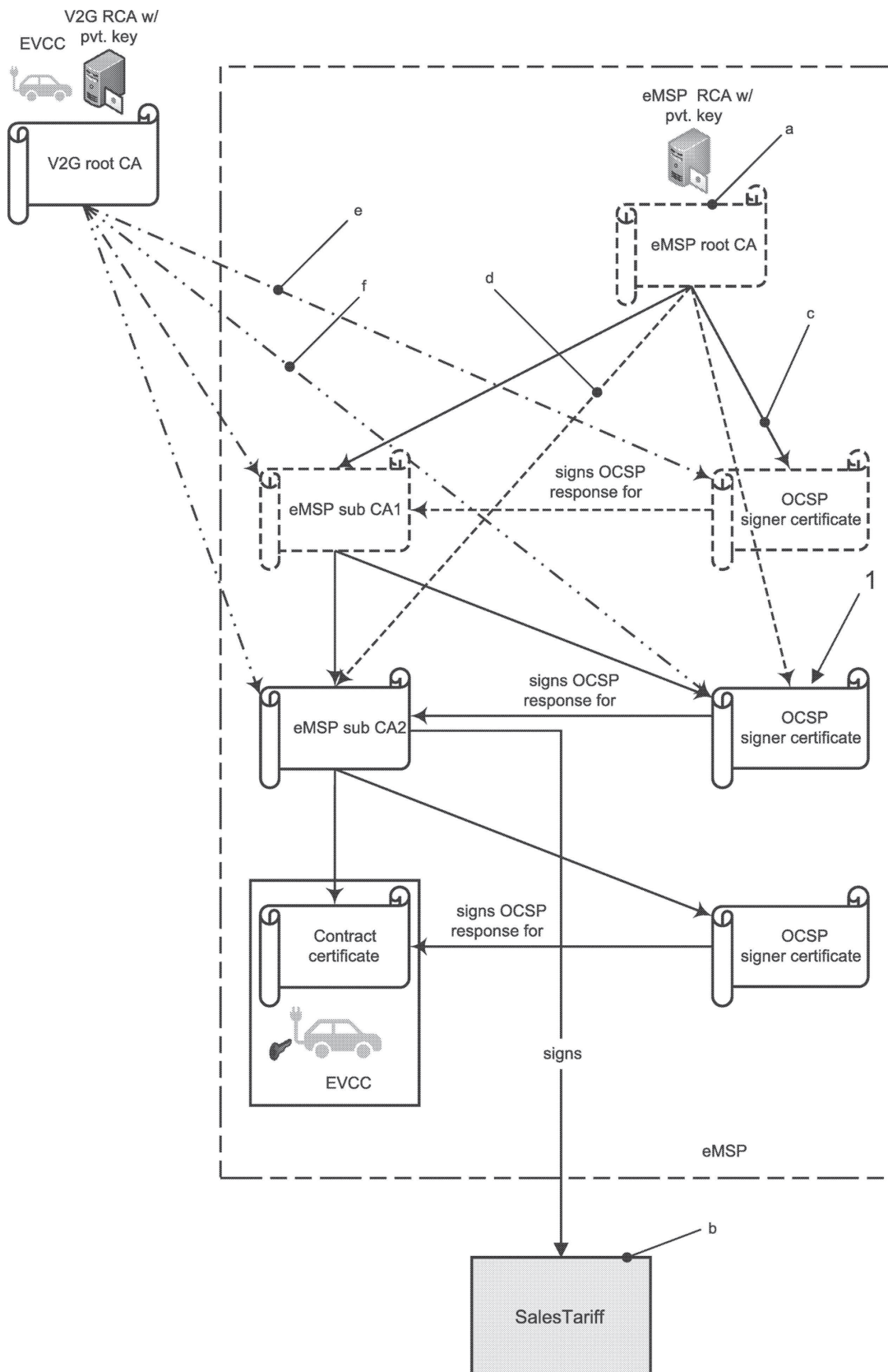
Figure 5 — Mandatory certificate structure originating from V2G root CA certificate

[V2G20-2329] A contract certificate shall be generated using a certificate chain that uses either an eMSP root CA certificate or a V2G root CA certificate as the trust anchor. Refer to Figure 6 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of a certificate structure. Refer to Annex B for details of the certificate profile.

NOTE 5 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the eMSP's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use (if any) as the trust anchor for their contract certificates.

[V2G20-2330] The OCSP signer certificate used to sign the OCSP response for contract certificate status shall be generated using a certificate chain that uses either an eMSP root CA certificate or a V2G root CA certificate as the trust anchor. Refer to Figure 6 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of a certificate structure. Refer to Annex B for details of the certificate profile.

NOTE 6 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the eMSP's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use (if any) as the trust anchor for the OCSP signer certificate that signs the OCSP response for their contract certificates.



Key

- 1 certificate
- ^a Optional certificate — If the sub-CA1 is not present, the sub-CA2 is signed by the V2G root CA.
- ^b SalesTariff is not a certificate. The black arrow does not depict a certificate signing or certificate derivation/origination. SalesTariff is data that is signed by the eMSP using the private key of the eMSP sub CA2.

Since, in a PnC use case, the EVCC always contains the eMSP sub-CA2 as part of its contract certificate chain, the EVCC always has the associated public key for eMSP sub-CA2 that it can use to verify the signatures on SalesTariff.

- c Direct certification — The use of sub-CA1 is optional.
- d Optional direct certification — If the sub-CA1 is present, it signs the sub-CA2 certificates.
- e Upon eMSP's discretion the contract certificate chain may originate from V2G root CA certificate. This type of arrow shows when the sub-CA1 is signed by the V2G root CA.
- f Upon eMSP's discretion the contract certificate chain may originate from V2G root CA certificate. This type of arrow shows when the sub-CA1 is not used and sub-CA2 is signed by the V2G root CA.

Figure 6 — Contract certificate structure

[V2G20-2331] A vehicle certificate shall be generated using a certificate chain that uses either an OEM root CA certificate or a V2G root CA certificate as the trust anchor. 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 7 In case the vehicle certificate is generated using a certificate chain that uses an OEM root CA certificate as the trust anchor, the issuer can consider to cross-sign the vehicle certificate chain (one of the sub-CAs in the vehicle certificate chain or the OEM root CA) by a V2G root CA certificate. This will improve availability of communications as specified in this document and allow the EV to utilize communications as specified in this document on any EVSE that supports the said V2G root CA regardless if the EVSE trusts the specific OEM root CA (i.e. has access to the specific OEM root CA certificate) or not.

NOTE 8 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the OEM's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use (if any) as the trust anchor for their vehicle certificates.

[V2G20-2332] The OCSP signer certificate used to sign the OCSP response for vehicle certificate status shall be generated using a certificate chain that uses either an OEM root CA certificate or a V2G root CA certificate as the trust anchor. 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 9 As in case of vehicle certificate, if the OCSP signer certificate that signs the OCSP response for the vehicle certificates is generated using a certificate chain that uses an OEM root CA as the trust anchor, the issuer can consider to cross-sign the OCSP signer certificate chain (one of the sub-CAs in the OCSP signer certificate chain or the OEM root CA) by a V2G root CA certificate. This will improve availability of communications as specified in this document and allow the EV to utilize communications as specified in this document on any EVSE that supports the said V2G root CA regardless if the EVSE trusts the specific OEM root CA (i.e. has access to the specific OEM root CA certificate) or not.

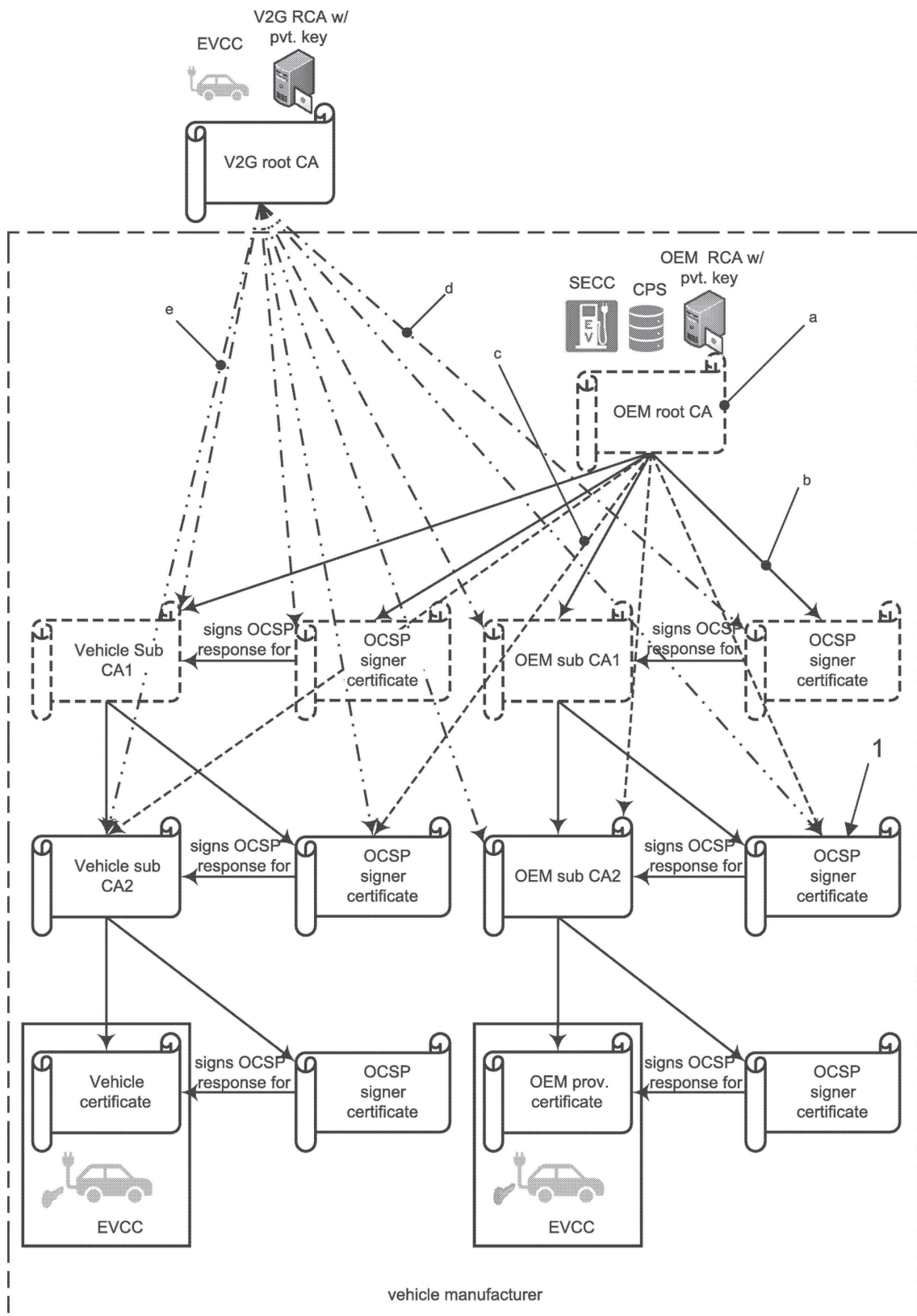
NOTE 10 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the OEM's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use (if any) as the trust anchor for the OCSP signer certificate that signs the OCSP response for their vehicle certificates.

[V2G20-2333] An OEM provisioning certificate shall be generated using a certificate chain that uses either an OEM root CA certificate or a V2G root CA certificate as the trust anchor. 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 11 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the OEM's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use (if any) as the trust anchor for their OEM provisioning certificates.

[V2G20-2334] The OCSP signer certificate used to sign the OCSP response for OEM provisioning certificate status shall be generated using a certificate chain that uses either an OEM root CA certificate or a V2G root CA certificate as the trust anchor. 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, it is up to the OEM's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use (if any) as the trust anchor for the OCSP signer certificate that signs the OCSP response for their OEM provisioning certificates.



Key

- 1 certificate
- ^a Optional certificate — If the sub-CA1 is not present, the sub-CA2 is signed by the V2G root CA.
- ^b Direct certification — The use of sub-CA1 is optional.
- ^c Optional direct certification — If the sub-CA1 is present, it signs the sub-CA2 certificates.
- ^d Upon OEM's discretion the vehicle certificate and OEM provisioning certificate chain may originate from V2G root CA certificate. This type of arrow shows when the sub-CA1 is signed by the V2G root CA.
- ^e Upon OEM's discretion the vehicle certificate and OEM provisioning certificate chain may originate from V2G root CA certificate. This type of arrow shows when the sub-CA1 is not used and sub-CA2 is signed by the V2G root CA.

Figure 7 — Certificate structure originating from OEM root CA certificate

[V2G20-2335] A PE certificate shall be generated using a certificate chain that uses a PE private root CA certificate as the trust anchor. 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.

[V2G20-2336] A PE certificate chain shall not be signed or cross-signed by any CA under a V2G root CA or an eMSP root CA or an OEM root CA. Similarly, PE certificate chain shall not be signed or cross-signed by any V2G root CA or eMSP root CA or OEM root CA.

NOTE 13 A PE certificate chain can, however, be cross-signed by a CA in another PE certificate chain.

7.3.2.1.1 Minimum required/mandatory certificates

Some certificates are needed for the functioning of this document. This subclause defines the minimum certificates required both in the SECC and the EVCC that allows basic communication to function. The basic function is defined as being able to setup the communication and utilize EIM for authorization of services. This subclause does not cover requirements for the private SECC.

[V2G20-2337] The SECC shall contain an SECC certificate. This certificate is necessary to establish a TLS session. Refer to 7.3.2.1 for SECC certificate requirements.

NOTE 1 In case of cross-signing the SECC certificate chain, the SECC can actually contain multiple sub-CA certificates and cross certificates.

[V2G20-2338] Each SECC shall possess at least one of either of the following root certificates:

- V2G root CA certificate;
- OR**
- OEM root CA certificate.

NOTE 2 This means that at any given time, the SECC can have at least one of the above valid root certificates. Since the vehicle certificate used during TLS session setup is based on at least one, if not both, of the root certificates mentioned here, an SECC cannot support communication without at least one of these roots.

NOTE 3 The SECC can possess more than one V2G root CA certificates.

NOTE 4 The SECC can possess more than one OEM root CA certificates.

NOTE 5 The SECC can possess both V2G root CA certificates and OEM root CA certificates.

[V2G20-2339] The EVCC shall contain a vehicle certificate. This certificate is necessary to establish a TLS session. Refer to 7.3.2.1 for vehicle certificate requirements.

NOTE 6 In case of cross-signing the vehicle certificate chain in the EVCC can actually contain multiple sub-CA certificates and cross certificates.

[V2G20-2340] The EVCC shall possess at least one V2G root CA certificate. This certificate is necessary to verify SECC certificates to establish TLS session. Refer to 7.3.2.1 for V2G root CA certificate requirements.