

DIN EN ISO 15118-2



ICS 43.120

Entwurf

Einsprüche bis 2019-01-23
Vorgesehen als Ersatz für
DIN EN ISO 15118-2:2016-08

**Straßenfahrzeuge –
Kommunikationsschnittstelle zwischen Fahrzeug und Ladestation –
Teil 2: Anforderungen an das Netzwerk- und Anwendungsprotokoll;
Englische Fassung prEN ISO 15118-2:2018, nur auf CD-ROM**

Road vehicles –
Vehicle to grid communication interface –
Part 2: Network and application protocol requirements;
English version prEN ISO 15118-2:2018, only on CD-ROM

Véhicules routiers –
Interface de communication entre véhicule et réseau électrique –
Partie 2: Exigences du protocole d'application et du réseau;
Version anglaise prEN ISO 15118-2:2018, seulement en CD-ROM

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2018-11-23 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 naaautomobil@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, 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.

Gesamtumfang 654 Seiten

DIN-Normenausschuss Automobiltechnik (NAAutomobil)

Nationales Vorwort

Dieses Dokument (prEN ISO 15118-2:2018) wurde vom Technischen Komitee ISO/TC 22 „Road vehicles“ ausgearbeitet, dessen Sekretariat von AFNOR gehalten wird, und wurde vom Technischen Komitee CEN/TC 301 „Straßenfahrzeuge“ übernommen, dessen Sekretariat von AFNOR (Frankreich) gehalten wird.

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

Der Entwurf ist derzeit zur parallelen Umfrage vorgelegt.

Das DIN-Präsidium hat mit seinem Beschluss 1/2004 festgelegt, dass von dem in den Regeln der europäischen Normungsarbeit von CEN/CENELEC verankerten Grundsatz, wonach Europäische Normen in den drei offiziellen Sprachen Deutsch, Englisch und Französisch veröffentlicht werden, in begründeten Ausnahmefällen abgewichen und auf die deutsche Sprachfassung verzichtet werden kann.

Die Genehmigung dafür hat die DIN-Geschäftsleitung entsprechend ihren in Anlage 1 zu dem DIN-Rundschreiben A 5/2004 festgelegten Kriterien für die vorliegende Norm auf Antrag des NA 052 NAAutomobil als Ergebnis einer Einzelfallentscheidung erteilt, zumal bereits dieser Norm zugrunde liegende Papiere überwiegend in englischer Sprache auch von den deutschen Marktteilnehmern angewendet werden.

Um den Energieverbrauch von Fahrzeugen zu senken, werden Fahrzeuge mit elektrischem Teil- oder Kompletantrieb 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 allgemeine Anforderungen an die Kommunikationsschnittstelle sowie die sicherheitsrelevanten Funktionen fest.

Änderungen

Gegenüber DIN EN ISO 15118-2:2016-08 wurden folgende Änderungen vorgenommen:

- a) die Anforderungen zur Kommunikation beim induktiven Laden wurden ergänzt;
- b) die Anforderungen zum Entladen der Fahrzeugbatterie wurden ergänzt;
- c) redaktionelle und formale Anpassungen.

Nationaler Anhang NA (informativ)

Begriffe

Die Benummerung der folgenden Begriffe und Abkürzungen ist identisch mit der Benummerung in der englischen Referenzfassung.

3 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

automatisches Verbindungsgerät

ACD

(en: automatic connection device)

Komponenten, die den automatischen Verbindungsprozess für den den kabelgebunden Energietransfer zwischen einem Elektrofahrzeug (EV) und der EV-Versorgungseinrichtung unterstützen

3.2

Grundladen

BC

(en: basic charging)

Ladephase während eines Ladevorgangs, die nur nach IEC 61851-1 Anhang A geregelt wird

3.3

BCB-Wechsel

(en: BCB Toggle)

eine wechselnde PWM-Signal Sequenz vom Zustand B nach C und wieder zurück in den Zustand B

3.4

Ladegrenzen

(en: charging limits)

Menge technischer Bedingungen (z. B. Spannung, Strom, Energie, Leistung), die während der Fahrzeug-zu-Ladesäule-Kommunikation (en: Vehicle-to-Grid, V2G) für einen Ladevorgang ausgehandelt werden

3.5

Lademodus

(en: charging session)

eine Art Dienstmodus angewendet auf Ladedienste

3.6

Kommunikationsstartzeitgeber

(en: communication setup timer)

Zeitgeber, der die Zeit D-LINK_READY.indication (DLINKSTATUS = LinkEstablished) bis zur Ladestartbotschaft überwacht

3.7

Vertragszertifikat

(en: contract certificate)

Zertifikat, welches zur Elektrofahrzeug-Kommunikationssteuerung (EVCC) von einer Unterzertifikatsbehörde des Messstellebetreibers (en: Meter Operator, MO) ausgestellt wird und in XML-Signaturen in den Anwendungsschichten verwendet wird, so dass eine Ladesäulen-Kommunikationssteuerung (SECC) oder ein nebenrangiger Akteur den Vertrag, der für die EVCC geschlossen wurde, bzw. Signaturen, die von der SECC ausgestellt wurden, überprüfen kann

3.8

Status Vorsteuerung

(en: control pilot state, CP state)

Vorsteuerungsstatus gemäß der Vorsteuerungsfunktion nach IEC 61851-1 Anhang A

3.9

Berechtigungsnachweis

(en: credentials)

Teilinformation, welche die Identität einer Einheit bestätigt

BEISPIEL Die Kombination aus einer Kontonummer und einem Passwort ist ein weitverbreitetes Beispiel für Berechtigungsnachweise.

3.10

hervorgehobene Verschlüsselungsregeln

DER

(en: Distinguished Encoding Rules)

Methode zur Verschlüsselung eines Datenobjektes, wie z. B. eines X.509-Zertifikats, welches digital markiert wird oder dessen Signatur verifiziert werden soll

3.11

dynamischer Steuerungsmodus

(en: dynamic control mode)

Informationen zum Steuerungsmodus für die Kommunikation findet man in ISO 15118-1 (Ed2). Die SECC steuert den Leistungsfluss und stellt der EVCC Sollwerte zur Verfügung, der sie folgt

3.12

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

3.13

flexibler Steuerungsmodus

(en: flexible control mode)

Steuerungsmodus für die Kommunikation

Anmerkung 1 zum Begriff: EVCC und SECC verhandeln ein Leistungsprofil für Lade- und Entladezwecke.

3.14

globale Adresse

(en: global address)

IP-Adresse mit uneingeschränktem Anwendungsbereich

3.15

übergeordnete Ladekommunikation

HLC-C

(en: high level communication charging)

Ladephase während eines Ladevorgangs, die nach ISO 15118 geregelt ist

3.16

Link-local-Adresse

(en: link-local address)

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

3.17

Identifizierungsmodus

(en: identification mode)

Authentifizierung und Autorisierung des Nutzerkontos

Anmerkung 1 zum Begriff: Ein Identifikationsmodus wird zur Identifizierungsauswahl verwendet. Mehrere Identifizierungsmodi decken dieselbe Dienstsequenz ab.

3.18

IP-Adresse

(en: IP address)

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

3.19

maximale Übertragungseinheit

MTU

(en: maximum transfer unit)

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

3.20

Botschaftsmenge

(en: message set)

Menge obligatorischer V2G-Kommunikationsbotschaften und -parameter für die EVCC oder SECC, welche ein oder mehrere Anwendungselement(e) abdeckt

3.21

Botschaftszeitgeber

(en: message timer)

Zeitgeber, der den Austausch eines Anfrage-Antwort-Paares überwacht

3.22

Multiplexkommunikation [MC]

(en: multiplex communication [MC])

Austausch mehrerer Botschaften mit unterschiedlichen Nutzdatentypen zwischen EV und EVSE über die V2GTP-Verbindung

3.23

Knoten

(en: node)

Gerät, welches IPv6 implementiert

3.24

Versorgungszertifikat der Fahrzeughersteller

(en: OEM provisioning certificate)

Zertifikat, welches für die EVCC ausgestellt wurde, damit die Bereitstellung eines Vertragszertifikates ermöglicht wird

3.25

Durchführungszeit

(en: performance time)

nicht-funktionale Zeitanforderung, die die Zeit festlegt, die eine V2G-Einheit während der Ausführung bestimmter Funktionalitäten nicht überschreiten darf

Anmerkung 1 zum Begriff: Dies ist ein fester Zeitwert.

3.26

private Umgebung

(en: private environment)

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

3.27

Neuverhandlung

(en: renegotiation)

Botschaftsaustausch zur Erneuerung der Übereinkunft des Ladezeitplans zwischen Elektrofahrzeug und Ladesäule während einer V2G-Kommunikationssitzung durch die Neuübertragung der Parameter SASchedule und ChargingProfile

3.28

Anfrage-Antwort-Botschaftspaar

(en: request-response message pair)

Anfragebotschaft mit entsprechender Antwortbotschaft

3.29

Anfrage-Antwort-Botschaftssequenz

(en: request-response message sequence)

vordefinierte Sequenz von Anfrage-Antwort-Botschaftspaaren

3.30

SDP-Client

(en: SDP client)

V2G-Einheit, die den SDP-Server (en: SECC Discovery Protocol, SDP) nutzt, um Konfigurationsinformationen über die Ladesäulen-Kommunikationssteuerung zu bekommen, um auf diese zugreifen zu können

3.31

SECC-Server

(en: SDP server)

V2G-Einheit, die Konfigurationsinformationen für den Zugriff auf die Ladesäulen-Kommunikationssteuerung liefert

3.32

SECC-Zertifikat

(en: SECC certificate)

Zertifikat, welches für die SECC von der Unterzertifikatsbehörde des Ladestationbetreibers (en: Charge Point Operator, CPO) (oder Hauptzertifikatsbehörde in einer privaten Umgebung) ausgestellt wurde, welches für TLS derart verwendet wird, dass die EVCC die Authentizität des SECC verifizieren kann

3.33

Sequenzzeitgeber

(en: sequence timer)

Zeitgeber, der eine Anfrage-Antwort-Botschaftssequenz überwacht

3.34

Dienstsitzung

(en: service session)

Menge von sequentiellen und kooperativen Aktivitäten verschiedener Leistungsübertragungstypen und anderen optionalen EVCC und SECC-Diensten, bestehend aus Botschaftsmengen mit eindeutigem Bezeichner

Anmerkung 1 zum Begriff: Ladesitzung und kalbellose Leistungsübertragungssitzung sind Arten von Dienstsitzungen.

3.35

Unterzertifikatsbehörde

(en: Sub-CA)

untergeordnete Zertifikatsbehörde, die z. B. SECCC-Zertifikate und/oder im Auftrag der Hauptzertifikatsbehörde Vertragszertifikate ausstellt, wie z. B. V2G-Hauptzertifikate oder Hauptzertifikate mobiler Betreiber (nur für E-Mobilitätskontenzertifikate)

Anmerkung 1 zum Begriff: Die Fähigkeit zur Ausstellung der Zertifikate wird von der V2G-Hauptzertifikatsbehörde übertragen und die V2G-Hauptzertifikatsbehörde kann diese Übertragung an die Unterzertifikatsbehörde jederzeit rückgängig machen.

3.36

Unterzertifikatsbehördenzertifikat

(en: Sub-CA certificate)

von der Unterzertifikatsbehörde ausgestelltes Zertifikat

3.37

TCP-Daten

(en: TCP_DATA)

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

3.38

Zeitüberschreitung

(en: timeout)

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

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

3.39

Zeitgeber

(en: timer)

Gerät oder Software zur Zeitmessung in einer Implementierung

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

3.40

private Umgebung

(en: private environment)

Für eine Nutzergruppe abgeschlossener Leistungsübertragungsdienst, der vom selben Dienstanbieter festgelegt wurde

3.41

V2G-Ladeschleife

(en: V2G charging loop)

V2G-Botschaftsphase zur Regelung des Ladeprozesses nach ISO 15118

3.42

V2G-Kommunikationssitzung

(en: V2G communication session)

Zuordnung von zwei spezifischen V2G-Einheiten für den Austausch von V2G-Botschaften

3.43

V2G-Einheit

(en: V2G entity)

primärer Akteur, der an der V2G-Kommunikation beteiligt ist und ein obligatorisches oder optionales Übertragungsprotokoll nach diesem Teil der ISO 15118 verwendet

Anmerkung 1 zum Begriff: Primäre Akteure können der EVCC oder SECC sein.

3.44

V2G-Botschaft

(en: V2G message)

Botschaft, die in der Anwendungsschicht ausgetauscht wird

Anmerkung 1 zum Begriff: Siehe Abschnitt 8 Application layer messages.

3.45

V2G-Konfiguration

(en: V2G setup)

Konfigurationsphase für den V2G-Botschaftsaustausch

3.46

V2G-Übertragungsprotokoll

(en: V2G transfer protocol)

Kommunikationsprotokoll für die Übertragung von V2G-Botschaften zwischen zwei V2G-Übertragungsprotokolleinheiten

3.47

V2GTP-Einheit

(en: V2GTP entity)

V2G-Einheit, die das V2G-Übertragungsprotokoll unterstützt

3.48

V2G-Hauptzertifikatsbehörde

(en: V2G root CA)

Zertifikatsbehörde (CA), welche Unterzertifikatsbehörden-Zertifikate an Unterzertifikatsbehörden ausstellt. Diese Unterzertifikatsbehörden sind dann angewiesen, entweder Zertifikate an eine zweite Unterzertifikatsbehörde (Sub-CA 2) auszustellen oder direkt Blattzertifikate, wie Vertragszertifikate oder SECC-Zertifikate, auszustellen

3.49

V2G-Hauptzertifikat

(en: V2G Root Certificate)

Zertifikat, welches von der Hauptzertifikatsbehörde ausgestellt wurde

3.50

kabellose Leistungsübertragungssitzung

WPT-Sitzung

(en: wireless power transfer session, WPT session)

Dienst, die auf WPT-Dienste angewendet wird

— Leerseite —

Contents

Page

1	Scope	9
2	Normative references	9
3	Terms and definitions	12
4	Symbols and abbreviated terms	16
5	Conventions	18
5.1	Definition of OSI based services	18
5.2	Requirement structure	18
5.3	Usage of RFC references	19
5.4	Notation used for XML schema diagrams	19
6	Document overview	19
7	Basic requirements for V2G communication	21
7.1	General information	21
7.2	Service primitive concept of OSI layered architecture	21
7.2.1	Overview	21
7.2.2	Syntax of service primitives	21
7.3	Security concept	22
7.3.1	General	22
7.3.2	Certificate and key management	26
7.3.3	Number of root certificates and root validity, certificate depth and size	28
7.3.4	Support and application of TLS	29
7.3.5	Firewall	30
7.4	V2G communication states and data link handling	31
7.5	Data link layer	37
7.6	Network layer	37
7.6.1	General	37
7.6.2	Applicable RFCs and limitations and protocol parameter settings	37
7.6.3	IP addressing	39
7.7	Transport layer	39
7.7.1	Transmission control protocol (TCP)	39
7.7.2	User datagram protocol (UDP)	40
7.7.3	Transport layer security (TLS)	40
7.8	V2G transfer protocol	44
7.8.1	General information	44
7.8.2	Supported ports	44
7.8.3	Protocol data unit	45
7.9	Presentation layer	49
7.9.1	XML and efficient XML interchange (EXI)	49
7.9.2	Message security	51
7.10	Application layer	58
7.10.1	SECC discovery protocol	58
7.10.2	Vehicle to grid application layer messages	65
7.10.3	Application layer service primitives	66
8	Application layer messages	69
8.1	General information and definitions	69
8.2	Protocol handshake definition	70
8.2.1	Handshake sequence	70
8.2.2	Message definition supportedAppProtocolReq and supportedAppProtocolRes	71
8.2.3	Semantics description supportedAppProtocol messages	71
8.2.4	Message examples	74
8.3	V2G message definition	75

8.3.1	Overview	75
8.3.2	Message definition	75
8.3.3	Message header definition.....	77
8.3.4	Message body definition.....	80
8.3.5	V2G request definition	81
8.3.6	V2G response definition	81
8.4	V2G communication session and body element definitions	81
8.4.1	General.....	81
8.4.2	Session handling	83
8.4.3	Common messages	89
8.4.4	AC messages	138
8.4.5	DC messages	143
8.4.6	WPT messages	154
8.4.7	ACD messages.....	181
8.4.8	BPT messages	193
8.5	Complex data types	205
8.5.1	Overview	205
8.5.2	Common	205
8.5.3	AC	262
8.5.4	DC	270
8.5.5	WPT	281
8.5.6	BPT	320
8.5.7	ACD	347
8.6	Service and message set selection	348
8.6.1	General.....	348
8.6.2	Selection of service and service parameters.....	349
8.6.3	Selection of message sets.....	361
8.6.4	Supported messages and parameters of message sets	365
8.7	V2G communication timing	368
8.7.1	Overview	368
8.7.2	Message sequence and communication session	370
8.7.3	Session setup and ready to charge	376
8.7.4	V2G message synchronization with IEC 61851-1 signalling	381
8.7.5	V2G message synchronization with IEC 61980-2 signalling	387
8.8	Message sequencing and error handling.....	388
8.8.1	Overview	388
8.8.2	Basic Definitions for Error Handling	388
8.8.3	ResponseCode handling.....	389
8.8.4	Request-response message sequence requirements	393
8.9	request-response message sequence examples	445
8.9.1	AC	445
8.9.2	DC	448
8.9.3	WPT	453
8.9.4	ACD	457
8.9.5	BPT	461
Annex A (normative)	Schema definition	470
A.1	Overview	470
A.2	V2G_CI_AppProtocol.xsd	471
A.3	V2G_CI_MsgDef.xsd.....	472
A.4	V2G_CI_MsgHeader.xsd	472
A.5	V2G_CI_MsgBody.xsd.....	472
A.6	V2G_CI_MsgDataTypes.xsd	484
A.7	xmldsig-core-schema.xsd.....	504
Annex B (normative)	Certificate profiles	508
Annex C (normative)	Specification of identifiers	516
C.1	e-Mobility Authentication Identifier (EMAID)	516
C.1.1	EMAID Syntax	516
C.1.2	EMAID Semantics	517

C.1.3	Calculation of the check digit	517
C.1.4	Usage of country codes	517
C.1.5	PCID structure	517
C.1.6	SECCID structure	518
C.2	Electric Vehicle Supply Equipment ID (EVSEID)	518
C.2.1	EVSEID Syntax	518
C.2.2	EVSEID Semantics	519
C.2.3	Usage of country codes	520
Annex D	(informative) Message sequencing for renegotiation	521
D.1	Overview	521
D.2	Renegotiation after resuming a V2G communication session	523
Annex E	(informative) Overview on XML signatures	525
E.1	Overview	525
E.2	Signature generation	525
E.3	Signature generation for secondary actors	528
E.4	Signature validation	528
Annex F	(informative) WPT message examples	530
F.1	Example of WPT message sequence	530
F.2	XML view of PairingReq for LPE	531
F.3	XML view of PairingRes for LPE	532
F.4	XML view of PairingReq for P2PS	533
F.5	XML view of PairingRes for P2PS	534
F.6	XML view of FinePositioningReq	535
F.7	XML view of FinePositioningRes	536
Annex G	(informative) ACD message examples	538
G.1	Enable SystemStatus messaging via a value added service selection	538
Annex H	(informative) Summary of requirements	543
Annex I	(Informativ)	562
Annex J	(Informativ)	563
Annex K	(informative) Mapping of Part 1 use case elements	564
K.1	Relation of Identification Modes and Use Case Elements	564
Annex L	(informative) Mapping of ISO 15118 message element names to SAE J2847/2 terms	601
L.1	SAE J2847/2 status codes	601
L.2	SAE J2847/2 Energy Transfer Types	602
L.3	SAE J2847/2 signals	603
Annex M	(informative) Message examples	604
M.1	Value Added Service selection	604
M.2	EXI encoded message examples	606
M.2.1	SessionSetupRes message	606
M.2.2	ChargeParameterDiscoveryReq message (AC-based)	606
M.2.3	CurrentDemandReq message	607
M.3	Schedules and tariff information	608
M.3.1	Overview	608
M.3.2	Dynamic GridSchedule w/o SalesTariff over ISO 15118 V2G CI	608
M.3.3	"Time Of Use"-based SalesTariff with constant value for GridSchedule	610
M.3.4	"Time Of Use"-based SalesTariff with dynamic GridSchedule	611
M.3.5	"Consumption"-based SalesTariff with constant value for GridSchedule	613
M.3.6	Multiple SalesTariffs with different Demand Limits in GridSchedule	614
M.3.7	Time of Use-based SalesTariffs including relativePricePercentage	616
Annex N	(informative) Application of certificates	627
N.1	General information	627
N.1.1	Overview	627
N.1.2	Demands of the OEM	628
N.1.3	Demands of the Secondary Actors	628

N.1.4	Rationale for Decisions in this Standard	629
N.1.5	Overview of the resulting certificate structure	630
N.2	Simplified certificate management in private environment	632
N.2.1	Overview (motivation)	632
N.2.2	Solution for private environments	632
N.2.3	Solution for emergency and disaster situations	635
N.3	Use of OEM provisioning certificates	636
N.3.1	Introduction	636
N.3.2	Processes	637
N.4	Security appliances and their associated certificates	639
Annex O	(informative) Encryption for the distribution of secret keys	642
O.1	Overview	642
O.2	Ephemeral-static Diffie-Hellman key agreement	642
O.3	Key pairs	643

Foreword

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

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

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

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

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

This second edition cancels and replaces the first edition (ISO 15118-2:2014), which has been technically revised.

The main changes compared to the previous edition are as follows:

- Includes corrections of errors and inconsistencies;
- Missing parts added;
- Applied changes to achieve a Unified XML Scheme supporting all charging modes and needs;
- Communication requirements on reserve power transfer added;
- Includes requirements in regard to wireless power transfer (included from ISO 15118-7).

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

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 electricity 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, specific charging infrastructure was 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, but it was assigned to ISO 15118 series came to be treated 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 may 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 (enables smoothing of the electricity load of the supply network for higher energy efficiency, and also provide power back to the grid (e.g. for grid services or acting as a standalone power supply as an emergency lifeline),
- * 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 2: Network and application protocol requirements

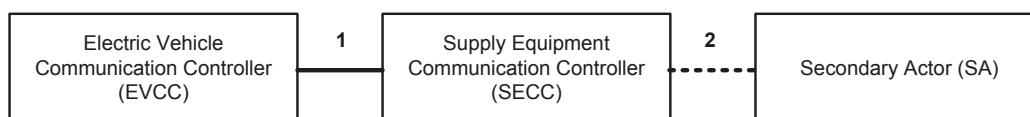
1 Scope

This international standard specifies the communication between the electric vehicle (EV), including battery electric vehicle (BEV) and plug-in hybrid electric vehicle (PHEV), and the EV supply equipment. The application layer message sets defined in this revision of ISO 15118-2 are designed to support the electricity power transfer between an EV and an EV supply equipment.

The bidirectional electricity power transfer, use case of that was already included in edition 1.0 of part 1 but not included in part 2, was officially added to the scope of this standard. Herein edition 2.0 of part 2 defines the communication messages and sequence requirements for bidirectional power transfer.

Also the scope is widely extended in this revision, requirements of wireless communication for both conductive charging and wireless charging are defined. Additionally, requirements of communication for automatic connection device and information services about charging and control status are defined in this revision.

The purpose of this part 2 of ISO 15118 is to detail the communication between an electric vehicle communication controller (EVCC) and 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 EVCC and SECC.



Key

- 1 Scope of ISO 15118-2
- 2 Message definition considers use cases defined for communication between SECC to SA

Figure 1 — Communication relationship among EVCC, SECC and secondary actor

This part 2 defines messages, data model, XML/EXI based data representation format, usage of V2GTP, TLS, TCP and IPv6. These requirements belong to the area of from 3rd to 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 a layer 3 perspective. The data link layer and physical layer functionality for wired communication is described in part 3 of this standard, and those of wireless communication are described in part 8 of this standard.

2 Normative references

The following referenced documents are required for the application 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 3166-1, *Codes for the representation of names of countries and their subdivisions — Part 1: Country codes*

ISO 15118-1, *Road vehicles — Vehicle to grid communication interface — Part 1: General information and use-case definition*

ISO 15118-3, *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

IEC 61851-1, Electric vehicle conductive charging system — Part 1: General requirements(Ed 2.0 2010)

IEC 61851-22, Electric vehicle conductive charging system - Part 22: AC electric vehicle charging station

IEC CDV 61851-23, Electric vehicle conductive charging system - Part 23: D.C. electric vehicle charging station (Ed 1.0 2012)

IEC 62196, Plugs, socket-outlets, vehicle connectors and vehicle inlets - Conductive charging of electric vehicles

IEC 61980-1, Electric vehicle wireless power transfer (WPT) systems - Part 1 General Requirements

IEC 61980-2, Electric vehicle wireless power transfer (WPT) systems - Part 2 specific requirements for communication between electric road vehicle (EV) and infrastructure with respect to wireless power transfer (WPT) systems

IEC61980-3, Electric vehicle wireless power transfer (WPT) systems Part 3: Specific requirements for the magnetic field wireless power transfer systemsISO 19363, Electrically propelled vehicles—Magnetic field wireless power transfer—Safety and interoperability requirements

SAE J2847-2 V4, Communication Between Plug-In Vehicles and Off-Board DC Chargers

W3C EXI 1.0, Efficient XML Interchange (EXI) Format 1.0, W3C Recommendation (March 2011)

W3C XML Signature Syntax and Processing Version 1.1, - W3C Recommendation (April 2013)

ISO 4130 Road vehicles -- Three-dimensional reference system and fiducial marks -- Definitions

IETF RFC 768, User Datagram Protocol (August 1980)

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

IETF RFC 1981, Path MTU Discovery for IP version 6 (August 1996)

IETF RFC 2460, Internet Protocol, Version 6 (IPv6) Specification (December 1998)

IETF RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (June 2013)

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

IETF RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6) (July 2003)

IETF RFC 3484, Default Address Selection for Internet Protocol version 6 (IPv6) (February 2003)

IETF RFC 6582, The NewReno Modification to TCP's Fast Recovery Algorithm (April 2012)

IETF RFC 4050, Using the Elliptic Curve Signature Algorithm (ECDSA) for XML Digital Signatures (April 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 5095, *Deprecation of Type 0 Routing Headers in IPv6* (December 2007)

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

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

IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2* (August 2008)

IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* (May 2008)

IETF RFC 5289, *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)* (August 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 6106, *IPv6 Router Advertisement Options for DNS Configuration* (November 2010)

IETF RFC 6961, *The Transport Layer Security (TLS) Multiple Certificate Status Request Extension* (June 2013)

IANA Service&PortRegistry, *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 Special Publication 800-56A: *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)* (March 2007)

NIST Special Publication 800-38A: *Recommendation for Block Cipher Modes of Operation - Methods and Techniques* (2001)

3 Terms and definitions

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

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

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

3.1

automatic connection device

ACD

components supporting the automatic connection and disconnection process for conductive energy transfer between an EV and EV supply equipment

3.2

basic charging

BC

charging phase during a charging session controlled by IEC 61851-1 Annex A only

3.3

BCB Toogle

a switching sequence of the PWM Signal from State B to C and back to State B

3.4

charging limits

a set of physical constraints (e.g. voltage, current, energy, power) that is negotiated during a service session

3.5

charging session

a kind of service session applied to charging services

3.6

communication setup timer

a timer monitoring the time D-LINK_READY.indication(DLINKSTATUS=LinkEstablished) until the Session Setup message

3.7

contract certificate

certificate issued for EVCC by a MO Sub-CA, which is used in XML signatures in application layer so that SECC or secondary actor can verify the contract issued to the EVCC and signatures issued by the EVCC

3.8

control pilot state

CP state

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

3.9

credentials

piece of information attesting an entity's identity

EXAMPLE The combination of an account number and a password is a widely used example of credentials.

3.10

distinguished encoding rules

DER

method for encoding a data object, such as an X.509 certificate, to be digitally signed or to have its signature verified

3.11

dynamic control mode

Control Mode for the Communication further Information can be found in ISO 15118-1 ED2NOTE The SECC controls the power flow and gives the EVCC Set Points it has to follow

3.12

elliptic curve cryptography

ECC

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

3.13

flexible schedule mode

Control Mode for the Communication further Information can be found in ISO 15118-1 ED2

Note 1 to entry: EVCC and SECC negotiate a power profile for Charging or Discharging purposes

3.14

global address

IP address with unlimited scope

3.15

high level communication charging

HLC-C

charging phase during a service session controlled by ISO 15118

3.16

link-local address

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

3.17

identification mode

authenticate and authorize the user account

Note 1 to entry: An identification mode is used for identification selection. Multiple identification modes cover same service sequence.

Note 2 to entry: Identification mode refers to EIM and PnC

3.18

IP address

address

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

3.19

maximum transfer unit

MTU

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

3.20

message set

set of V2G messages and parameters for the EVCC or SECC covering one or multiple use case elements

ISO/DIS 15118-2:2018(E)
ISO/DIS 15118-2 ED2**3.21****message timer**

timer monitoring the exchange of a request-response-pair

3.22 Multiplexed Communication [MC]

exchange of multiple messages with different payload types over the V2GTP connection between EV and EVSE

3.23**node**

device that implements IPv6

3.24**OEM provisioning certificate**

certificate issued to the EVCC to enable the provisioning of a contract certificate

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

3.25**performance time**

non-functional timing requirement defining the time a V2G Entity doesn't exceed when executing or processing certain functionality

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

3.26**private environment**

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

3.27**renegotiation**

messaging for updating the agreement on the charging schedule between EV and EV supply equipment during a V2G communication session by retransmitting the parameters SASchedule and ChargingProfile

3.28**request-response message pair**

request message and the corresponding response message

3.29**request-response message sequence**

a predefined sequence of request-response message pairs

3.30**SDP client**

V2G entity that uses the SDP server to get configuration information about the SECC to be able to access the SECC

3.31**SDP server**

a V2G entity providing configuration information for accessing the SECC

3.32**SECC certificate**

certificate issued to SECC by a CPO Sub-CA (or PE Root CA in a private environment), which is used in TLS so that the EVCC can verify the authenticity of the SECC

3.33

sequence timer

timer monitoring a request-response message sequence

3.34

service session

set of sequential and cooperative activity for various types of power transfer and other optional services by EVCC and SECC consists of message sets with unique ID

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

3.35

Sub-CA

subordinate certificate authority who issues e.g. SECC certificates and/or contract certificates on behalf of a root CA such as V2G root CA or mobility operator root CA (only for E-Mobility Accountcertificates)

Note 1 to entry: The ability of issuing the certificates are delegated from V2G root CA, and V2G root CA can revoke the Sub-CA at any time.

3.36

Sub-CA certificate

certificate issued to Sub-CA

3.37

TCP_DATA

socket/interface for data transfer based on TCP connection

3.38

timeout

timing requirement defining the time a V2G entity monitors the communication system for a certain event to occur

Note 1 to entry: If the specified time is exceeded the respective V2G entity initiates the related error handling. This is a fixed time value.

3.39

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 as well.

3.40

private environment

closed power transfer service for user group defined by the same service provider

3.41

V2G charging loop

V2G messaging phase for controlling the charging process by ISO 15118

3.42

V2G communication session

association of two specific V2G entities for exchanging V2G messages

3.43

V2G entity

primary actor participating in the V2G communication using a transmission protocol defined by this part of ISO 15118

Note 1 to entry: Primary actors can be EVCC or SECC.

ISO/DIS 15118-2:2018(E)
ISO/DIS 15118-2 ED2**3.44****V2G message**

message exchanged on application layer

Note 1 to entry: Refer to clause 8 Application layer messages

3.45**V2G setup**

setup phase for V2G messaging

3.46**V2G transfer protocol**

communication protocol to transfer V2G messages between two V2GTP entities

3.47**V2GTP entity**

V2G entity supporting the V2G transfer protocol

3.48**V2G root CA**

certificate authority (CA) who issues Sub-CA certificates to Sub-CAs. Those Sub-CAs are then delegated to issue either certificates to a second Sub-CA (Sub-CA 2) or to directly issue leaf certificates, such as contract certificate or SECC certificates

3.49**V2G root certificate**

certificate issued by V2G root CA

3.50**wireless power transfer session****WPT session**

kind of service session applied to WPT service

4 Symbols and abbreviated terms

For the purposes of this document, the following abbreviations apply:

AC	alternating current
BEV	battery electric vehicle
BPT	bidirectional power transfer
CA	certificate authority
CRL	certificate revocation list
DC	direct current
DH	Diffie Hellman
DER	distinguished encoding rules
ECDSA	elliptic curve digital signature algorithm

EMA	E-Mobility Account
EMAID	E-Mobility Authentication Identifier
EMOCH	E-Mobility operator clearing house (see also 15118-1, [12])
EV	electric vehicle
EVCC	electric vehicle communication controller
EVRESS	electric vehicle rechargeable energy storage system
EVSE	electric vehicle supply equipment
NOTE	EV supply equipment is used in description according to IEC 61851-1. EVSE is applied only for parameter name or message definition.
EXI	efficient XML interchange
OCSP	online certificate status protocol
OEM	original equipment manufacturer
NACK	negative acknowledgement
PDU	protocol data unit
PHEV	plug-in hybrid electric vehicle
PKI	public key infrastructure
PLC	power line communication
PnC	Plug and Charge/Park and Charge
PPD	Pairing and Positioning Device
RFC	Request for Comments(IETF)
RMS	root mean square
RPT	Reverse Power Transfer
SA	secondary actor
SDP	SECC discovery protocol
SDU	service data unit
SECC	supply equipment communication controller
TCP	transmission control protocol
UDP	user datagram protocol
VAS	Value Added Service
V2G	vehicle to grid communication

ISO/DIS 15118-2:2018(E)
ISO/DIS 15118-2 ED2

V2G CI	vehicle-to-grid communication interface
V2GTP	V2G transfer protocol
WPT	wireless power transfer
XML	extensible markup language

5 Conventions

5.1 Definition of OSI based services

ISO 15118-2 is based on the conventions defined in the OSI service conventions (refer to ISO 10731) as they apply for the individual layers specified in this document.

This part of ISO 15118-2 describes requirements applicable to layer 3-7 according to the OSI layered architecture.

5.2 Requirement structure

This document uses requirement structure defined here. 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 1st format is applied for new defined and updated requirements:

[V2G2-ED2-xxxx] requirement text, where;

- ‘V2G2’ represents the ISO 15118-2, second part of this standard sets.
- ‘ED2’ represents the second edition of this standard.
- ‘xxxx’ represents the unique requirement number consisting of four digits starts from 1000.
- ‘requirement text’ defines the actual text of the requirement.

EXAMPLE [V2G2-ED2-1000] This shall be an example requirement introduced in second edition.

The next 2nd format is applied to the handed over requirements from first edition of this document:

[V2G2-ED2-yyy] requirement text, where;

- ‘V2G’ represents the ISO 15118-2, second part of this standard sets.
- ‘ED2’ represents the second edition of this standard.
- ‘yyy’ represents the unique requirement number same as defined in first edition.
- ‘requirement text’ is the same text as defined in first edition.

EXAMPLE [V2G2-ED2-000] This shall be an example requirement originally defined in first edition.

NOTE More information about requirements is provided in Annex M.

5.3 Usage of RFC references

When RFCs are referenced by requirements, latest version will be applied.

[V2G2-ED2-1230] All published updates and error corrections shall be applied to the referred RFC.

5.4 Notation used for XML schema diagrams

This standard 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 Altova XMLSpy Manual.

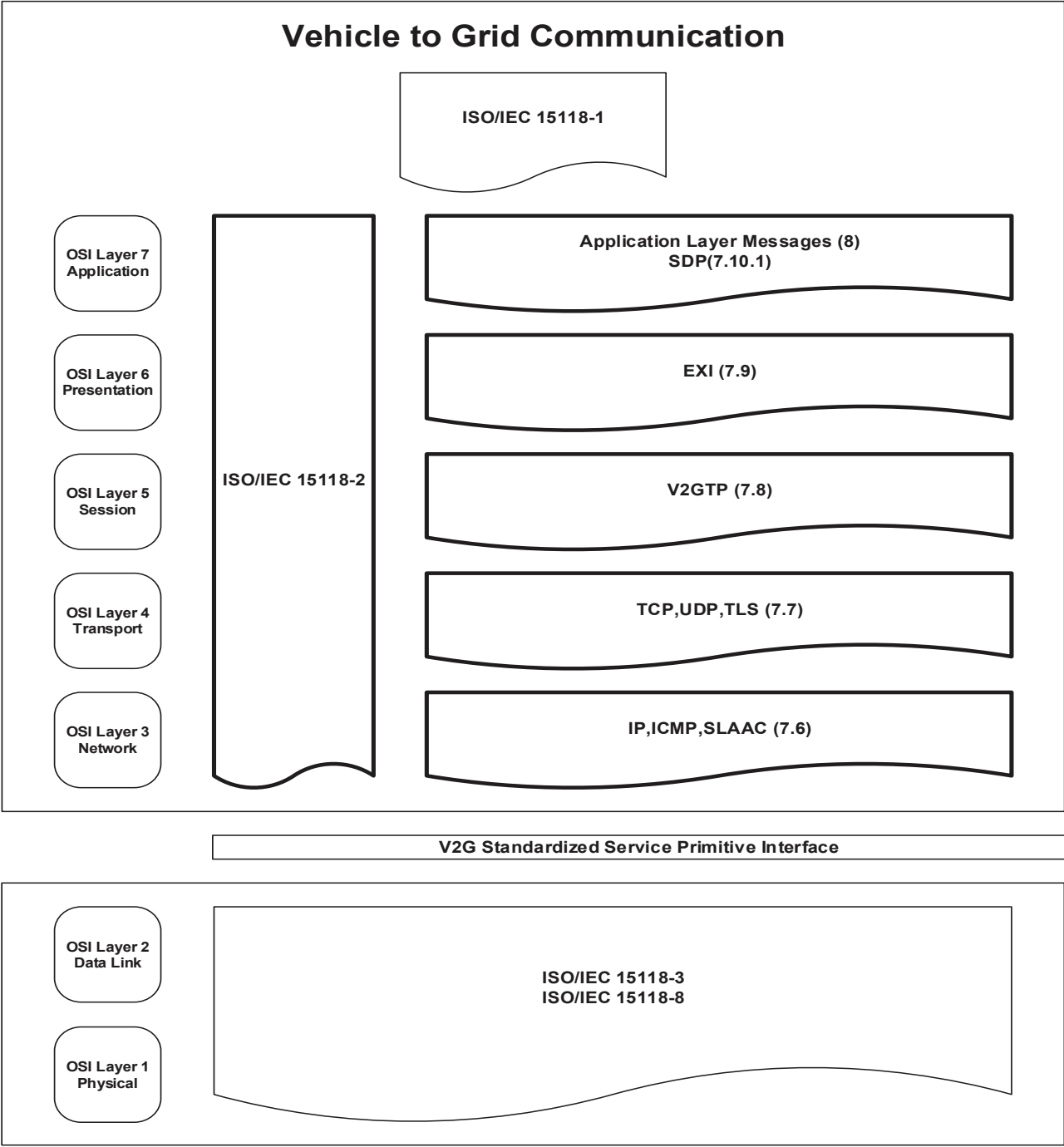
Allowing for an easy way to distinguish the types used for the XML schema definitions in this standard following naming conventions apply:

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

6 Document overview

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

As indicated by the bold framed shapes this Part of ISO 15118 defines requirements applicable to layers 3-7 according to the OSI layered architecture. Layer 1 and 2 requirements including the V2G Standardized Service Primitive Interface are specified in ISO 15118-3 and ISO 15118-8.



Key

-  OSI Layers and applicable requirements described in this Part of ISO 15118
-  OSI Layers and applicable requirements defined in other Parts of ISO 15118

Figure 2 — Vehicle to grid communication document overview

7 Basic requirements for V2G communication

7.1 General information

This Part of ISO 15118 describes the realization of the V2G use cases elements defined by Part 1 of this standard.

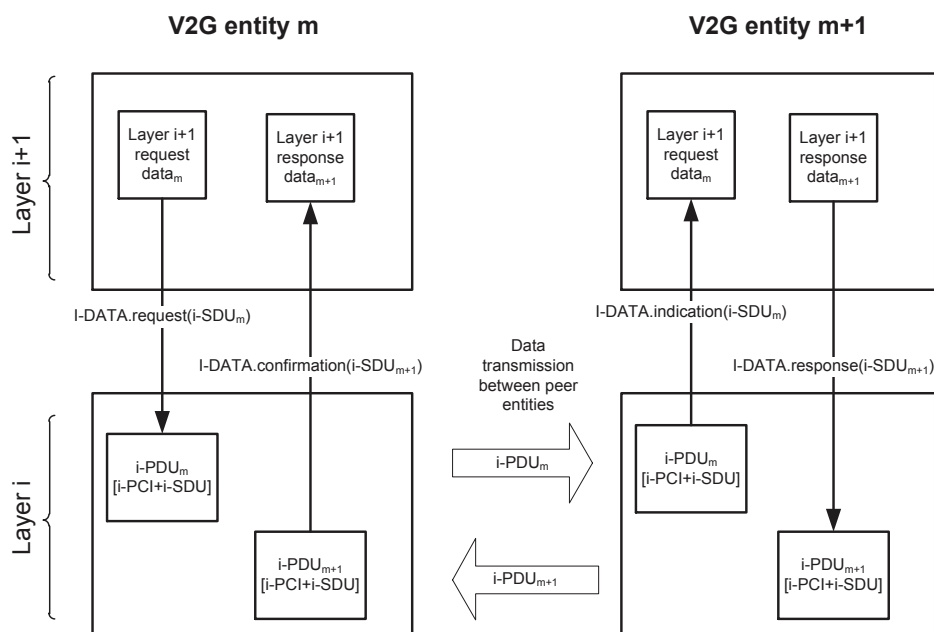
7.2 Service primitive concept of OSI layered architecture

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)

ISO/DIS 15118-2:2018(E)
ISO/DIS 15118-2 ED2

— whereas [initial of layer] is one out of the following seven:
[Physical, Data Link, Network, Transport, Session, Presentation, Application]

— whereas [NAME] is the name of the primitive

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

— whereas [primitive type] is one out of the following four:
[request, indication, response, confirmation]

— 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

In ISO 15118-2 first edition, TLS was not mandatory for all message sets. In ISO 15118-2 second edition, TLS is mandatory for all message sets. "For the backward compatibility, connection setup processes will accept both first edition and second edition handling. This means connection setup processes will be not changed. After the confirmation of software version between EVCC and SECC, established connection will be confirmed or stopped.

If some of application still requires optional TLS, first edition of this standard will be applied.

Figure 4 and Figure 5 depict the principal approach for the semi-online and the online case from a security point of view, showing the necessary security services applied as well as an abstract view on the different data necessary for the operation.

The full data flow / sequence charts can be found in subclause 8.8 of this document. In Figure 4 and Figure 5 only the security relevant information shall be highlighted.

The security concept provides a basic transport based protection mechanism. For all scenarios of Edition 2, the usage of Transport Layer Security (TLS) for the transport communication between EVCC and SECC is mandatory. In case data has to be protected from or to a secondary actor or if the protection has to last longer than the existence of the TLS channel, specific messages could be protected on application layer (XML-messages).

Figure 4 shows an example sequence for a semi-online connection for a PnC scenario.

In this PnC example, all TCP/IP based communication is protected using a unilaterally authenticated TLS channel between the two peers.

All communication is terminated at the SECC. The meter reading is cyclically signed by the vehicle to support the billing process (refer to 8.4.3.13.1). This information may be used for billing if local regulations permit it. The EV supply equipment provides the charging records which contain the signed meter reading to the backend for further processing.

NOTE 1 The communication between SECC and SA in Figure 4 is shown for informational purpose only and not intended to specify a particular message sequence.

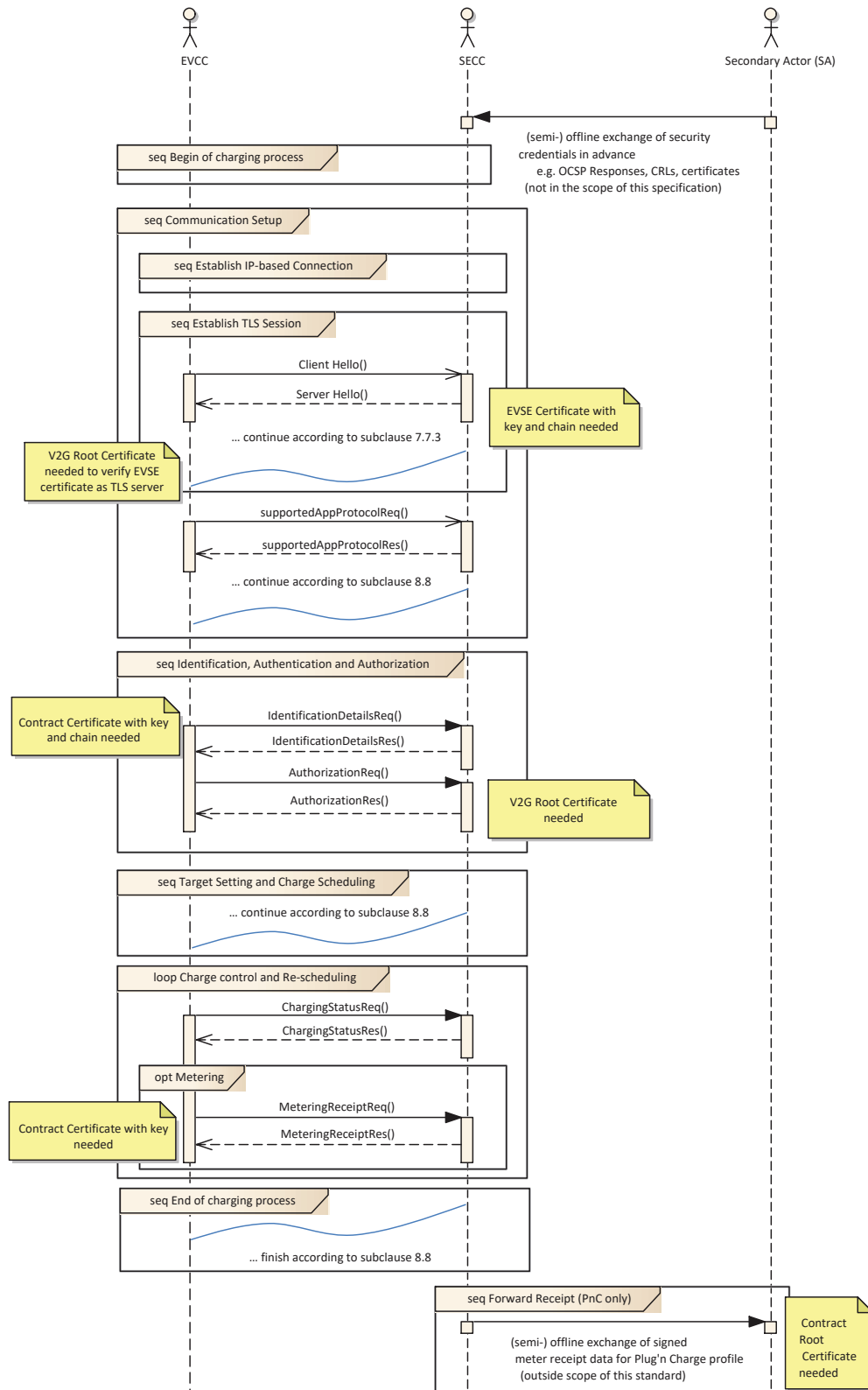


Figure 4 — Example for semi-online call flows

Figure 5 shows an example sequence for an online PnC scenario.

As described in Figure 5, all TCP/IP based communication is protected using a unilaterally authenticated TLS channel between the two peers.

ISO/DIS 15118-2:2018(E)
ISO/DIS 15118-2 ED2

Some of the information provided by the EVCC may need to be sent to the SA for further processing, like the EMAID or the EVCC credentials to be able to sign the tariff information. The EVCC calculates a charging profile (refer to subclause 8.4.3.9.2) and sends it to the SECC. The SECC may send it to SA systems like Smart Grid or Demand Clearing House. The 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 2 The communication between SECC and SA in Figure 5 is shown for informational purpose only and not intended to specify a particular message sequence.

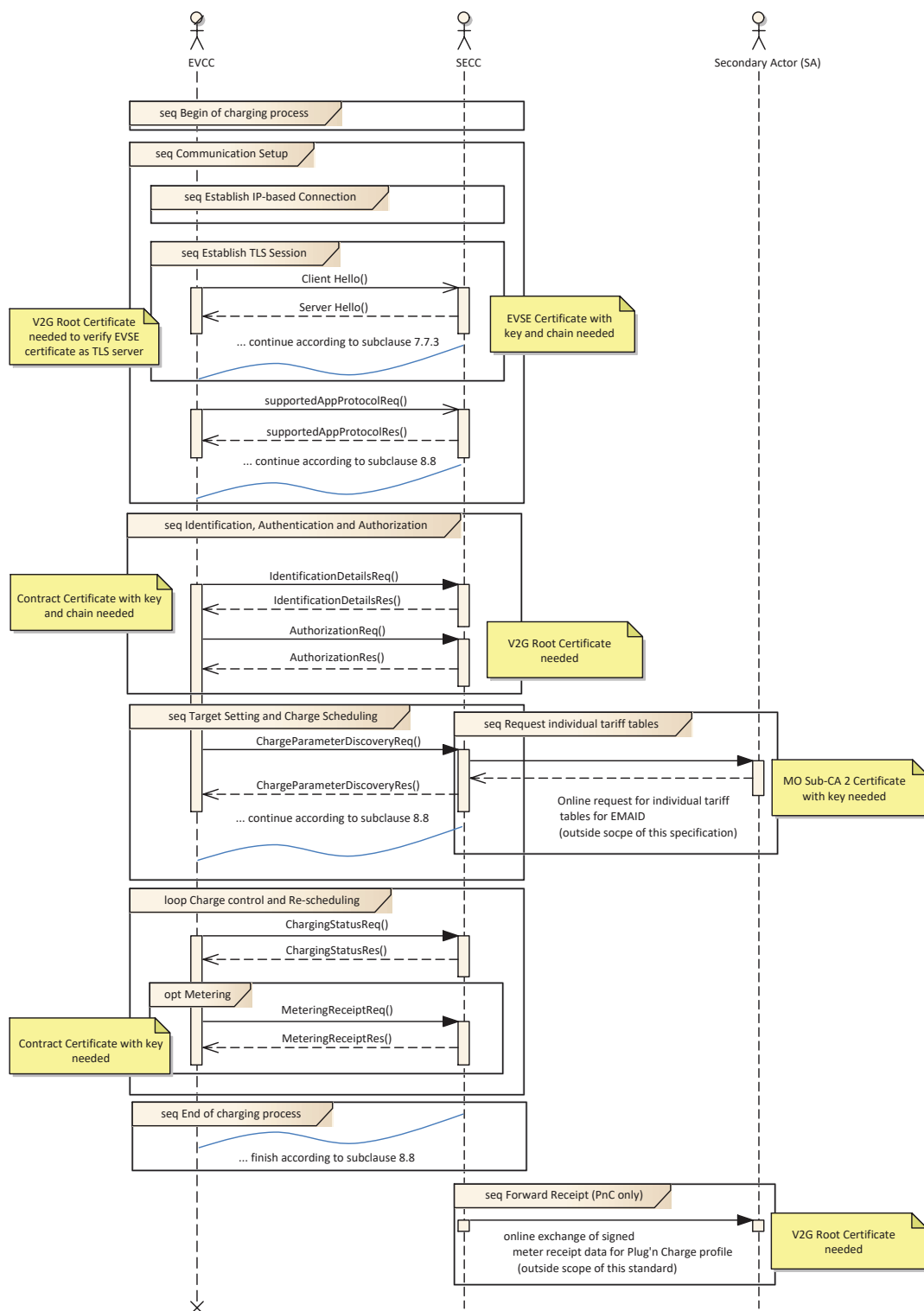


Figure 5 — Example for online call flows

There are further use cases where security mechanism are needed on application layer. These are the initial enrollment of contract keys and certificate as well as the update of the certificate. In this case vehicle specific OEM keys are used. Those mechanisms are described in Annex N.3. An overview on all needed certificates can be found in Annex B.

ISO/DIS 15118-2:2018(E)
ISO/DIS 15118-2 ED2

7.3.2 Certificate and key management

The call flows shown in clause 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 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 Certificates and possibly Sub-CA Certificates which certify SECC Certificates and Contract Certificates.

Separate from above certificates, there may be OEM Root Certificates and OEM Provisioning Certificates to be used for installing and updating Contract Certificates.

For an overview over all possible certificate profiles, see Annex B.

[V2G2-ED2-1231] Each V2G Entity shall use X.509v3 certificates.

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

Table 1 — Basic certificate fields

Certificate field	Description
Version	Version of certificate (for 15118 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	Optional (see Table 2)
Signature	Signature of the certificate generated by the issuer

NOTE 1 For those not familiar with the various fields refer to IETF RFC 5280.

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	Further specification of key usage using OIDs, e.g.: Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Note, sometimes here also the following values are encoded: Netscape SGC (1.3.6.1.4.1.311.10.3.3) Microsoft SGC (2.16.840.1.113730.4.1) SGC stands for Server Gated Crypto and indicated that the server may also use strong cryptography for the connection with the client's browser. This extension was used at the time of strong crypto export control to enable financial web site to provide appropriate protection of the data transfer.
CRL distribution point	Location to retrieve certificate revocation lists
OCSP	Location to retrieve OCSP. Refer to IETF RFC 6960 for details.
Authority information	Additional authorization information
Subject alternative name	Alternative names of the entity
Basic constraint = CA	True if the certificate is V2G Root Certificate or SubCA certificate.

NOTE 2 For those not familiar with OIDs, e.g. 1.3.6.1.5.5.7.3.1, refer to: Object Identifier (OID) Repository.

[V2G2-ED2-005] Each V2G Entity shall support Hash-operation SHA-256 (signature process) according to NIST FIPS PUB 180-4 (for ISO 15118-1 Use Case Element ID: F1).

[V2G2-ED2-006] For each V2G Entity the signature operation shall be ECC-based using elliptic curves (secp256r1[SECG notation]) with signature algorithm ECDSA (for ISO 15118-1 Use Case Element ID: F1).

[V2G2-ED2-1000] Both, the r- and the s-value shall always be transferred with their maximum length. If any of these values is shorter, it shall be filled up with leading zeros. The receiver shall assign the first half of the bytes to r and the second half of the bytes to s. This encoding is described in detail in section 3.3 of [RFC4050].

NOTE 3 The r and s value are the output of the ECDSA(Elliptic Curve Digital Signature Algorithm) and consist of a pair of integers.

[V2G2-ED2-007] The key length for ECC based asymmetric cryptography each V2G Entity uses shall be 256 bit.

[V2G2-ED2-885] All certificate validations shall be carried out in conformance with RFC 5280. For every certificate profile in Annex F, every critical KeyUsage attribute shall be checked in case it is set to the value 1. All BasicConstraints attributes shall be checked as well. The EVCC and the SECC may cache certificate validation results during one charging session.

[V2G2-ED2-926] The certificate extensions mentioned in Annex B shall be supported. Deviations are specified where necessary.

[V2G2-ED2-925] A leaf certificate shall be treated as invalid, if the trust anchor at the end of the chain does not match the specific root certificate required for a certain use, or if the required Domain Component value is not present.

[V2G2-ED2-1232] The EVCC shall provide a mechanism to check the validity periods of certificates and OCSP responses.

[V2G2-ED2-1233] The EVCC shall respect the chosen accuracy when using the time source. The accuracy shall be maximum one day.

NOTE 4 This requirement theoretically even allows for precisions of e.g. one year. The implementer should carefully weigh the security consequences of such a decision.

[V2G2-ED2-887] The SECC shall ensure that at any point in time it has a certificate for itself, which is valid for at least one more hour.

7.3.3 Number of root certificates and root validity, certificate depth and size

[V2G2-ED2-008] Each EVCC shall support at least two V2G root certificate.

NOTE Storing two V2G root certificates is required to be able to store the currently valid V2G root certificate of a specific V2G root CA and additionally the new V2G root certificate of that V2G root CA that will be valid after the previous V2G root certificate has expired.

[V2G2-ED2-877] Each SECC shall support the storage of at least 10 V2G root certificates.

NOTE 1 Due to overlapping validity periods, up to 10 concurrently valid certificates may exist. See **[V2G2-ED2-1517]**

NOTE 2 Five (5) number of V2G root certificates for the EVCC are strongly recommended. However, just one is mandatory. Having less than 5 or just 1 certificate brings a risk to the OEM. Having just 1 V2G root certificate allows the EV to charge just in that one region. The OEM will need to state in the manual and during offering the EV to customers, that this EV charges only in its "home" region. If an OEM is afraid, that 5 V2G root certificates are not sufficient to cover the "usage radius" of its EVs, OEM is free to provide more root certificate storage locations.

NOTE 3 It is assumed that the V2G Root Certificates applied on OSI layer 4 are also used on OSI layer 7. Additionally it is assumed that in Europe there will be a single root certificate authority similar to the Trust Center that was established for the EURO5/EU5. It is also assumed that other regions of the world will also manage to have a root certificate authority covering a greater number of actors. This leads to the assumption that 5 root certificates for 5 world-regions are sufficient. If one decides for more space for certificates this doesn't affect compatibility.

[V2G2-ED2-009] The path length constraint of the PKI certificate tree shall be limited to 3.

NOTE 4 The path length constraint defines the number of non-self-signed certificates in a certification path, i.e. there will be up to 3 certificate layers derived from the root certificate.

[V2G2-ED2-1234] Certificates shall be DER encoded and the size of a certificate in DER encoded form shall be limited to 800 bytes.

[V2G2-ED2-1517] All providers of certificates shall be responsible to ensure the certificate's validity for the lifetime of the trust relationship, e.g. between EVCC and SECC. **[V2G2-ED2-867]** A V2G root shall not issue a leaf certificate.

NOTE 6 Leaf certificates can only be issued by a Sub-CA.

[V2G2-ED2-869] No CA or Sub-CA shall issue and sign a certificate which is valid for longer than the validity period of itself as the signing entity.

[V2G2-ED2-911] 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-CA 2 shall apply for that Sub-CA.

The following requirements enable simplified certificate handling within Private Environments. See Annex N.2 for a more detailed explanation.

[V2G2-ED2-882] Each EVCC shall be able to store at least one Private Operator Root Certificate which shall be replaceable by the car owner.

[V2G2-ED2-927] The EVCC shall consider stored Private Operator Root Certificates as trust anchors for SECC Certificate verification.

NOTE 7 The validity times of SECC certificates having a trusted private operator root certificate as their trust anchor is chosen by the certificate signer at his own discretion.

NOTE 8 For a private environment, sub-CAs and OCSP responses are not supported.

NOTE 9 That means, a private operator root certificate directly signs a leaf certificate.

7.3.4 Support and application of TLS

According to sub-clause 7.3.2 and 7.3.3, this document requires following TLS managements;

- 1) The certificate managements defined in sub-clause 7.3.2
- 2) The key managements defined in sub-clause 7.3.2
- 3) The certificate chain structure defined in sub-clause 7.3.3
- 4) The certificate validity period defined in sub-clause 7.3.3

TLS with these features is defined as V2G-CI-TLS in this document. In first edition of this document, usage of V2G-CI-TLS wasn't mandatory for all message sets. But in this second edition, it is changed to be mandatory for all message sets.

[V2G2-ED2-1238] SDP handshake shall be applied according to Table 3.

[V2G2-ED2-1235] V2G-CI-TLS shall be applied to all message sets for both EVCC and SECC, if the chosen ProtocolNamespace is equal to "urn:iso:std:iso:15118:-2:ed-2"..

NOTE 1 In stand-alone application without internet connections, OCSP is not possible.

NOTE 2 If V2G-CI-TLS is not available for various reasons, the security scheme authorized by local responsibility is recommended to be applied.

After the message exchange of supportedAppProtocolReq/Res, usage of V2G-CI-TLS shall be confirmed.

[V2G2-ED2-1237] If the established connection between EVCC and SECC is TCP without TLS and the ProtocolNamespace that was chosen is equal to "urn:iso:std:iso:15118:-2:ed-2", the SECC shall stop TCP connection between EVCC and SECC.

According to the first edition of this document, establishment of connection between EVCC and SECC is defined in Table 3.

The support, usage and restrictions regarding TLS are described in Table 3.

Table 3 — SDP handshake between EVCC and SECC

EVCC TLS support	SECC TLS support	SDP request by EVCC	SDP response SECC
EVCC has TLS support	SECC has TLS support	EVCC signals TLS	SECC shall respond TLS
		EVCC signals TCP	SECC shall respond TCP
	SECC has no TLS support	EVCC signals TLS	SECC can indicate that it does not support TLS with indicating "0x10 = No transport layer security" in its SDP response. The EV can decide if it wants to continue TCP without TLS, or otherwise stop the communication setup.
		EVCC signals TCP	SECC shall respond TCP
EVCC has no TLS support	SECC has TLS support	EVCC signals TCP	SECC shall respond TCP
	SECC has no TLS support	EVCC signals TCP	SECC shall respond TCP

NOTE 3 This table is same as the definition for private environment in first edition. In the general environment, SECC always responds with TCP to TCP and with TLS to TLS request from EVCC. So connection support in general environment is the part of that of private environment.

Private environment is the power transfer service for closed user group. User group is defined and managed by service provider of power transfer service itself and the security of the field for providing service is managed by it according to its security policy, so the authentication for SECC by EVCC through TLS connection might be negligible.

Example 1 members of car sharing system using RFID token

Example 2 energy power transfer connecting HEMS network in a home garage

Example 3 EV taxi charging within a management of taxi company

7.3.5 Firewall

This section defines firewall functionality, where the term firewall refers to the definition made in ISO/IEC 27033-1:2015. The firewall specified here separates the trusted from the untrusted network, where trusted and untrusted are defined as follows:

Trusted network SECCs and SDP servers are part of the trusted network. Access to this network is controlled by the EV supply equipment operator. Only authorized nodes of the operator have access to this network.

Untrusted network EVCCs are part of the untrusted network. Access to this network is not controlled by the EV supply equipment operator.

[V2G2-ED2-1013] When using wireless communication according to 15118-8, there shall be at least one firewall between the EVCC which is connected to an untrusted network and the SECC, which is connected to a trusted network.

[V2G2-ED2-1014] For security reasons the rules mentioned in Table 4 shall apply for the firewall mentioned in [V2G2-ED2-1013].

Table 4 Firewall action for wireless communication

Source		Destination		Protocol	Interface		Action
IP Address	Port	IP Address	Port		Inbound	Outbound	
all	EVCC Port (dynamic range)	ff02::01	15118	UDP	untrusted	trusted	allow
all	EVCC Port (dynamic range)	SECC IP Address	SECC Port (V2G_DST_TCP_DATA)	TCP	untrusted	trusted	allow
all	EVCC Port (dynamic range)	SECC IP Address	1080	TCP	untrusted	trusted	allow
SDP Server IP Address	15118	EVCC IP Address	EVCC Port	UDP	trusted	untrusted	allow
SECC IP Address	SECC Port (V2G_DST_TCP_DATA)	EVCC IP Address	EVCC Port	TCP	trusted	untrusted	allow
SECC IP Address	1080	EVCC IP Address	EVCC Port	TCP	trusted	untrusted	allow
SECC IP Address	SECC Port [SECC_VAS_Port]	EVCC IP Address	EVCC Port	TCP	trusted	untrusted	allow
all	all	all	all	all	trusted	trusted	allow
all	all	all	all	all	all	all	deny

NOTE Allow means to establish connetion and deny means Port-unreachacle for the Source.

7.4 V2G communication states and data link handling

V2G messaging on application layer requires the establishment of the lower layer protocols to enable V2G message exchange between EVCC and SECC. This document focuses on protocols above the Data-Link layer. The data link layer is described in ISO 15118-3.

This subclause defines the basic requirements for establishing communication above the data link layer. The standard does not imply any implementation. The figures in this chapter only show the basic sequencing for managing the protocol stack.

The timer, timeout and performance time values used in this subclause are described in subclause 8.8 .

Figure 6 depicts the general communication states of the V2G communication from an EVCC perspective.

The following applies for the EVCC:

[V2G2-ED2-014] After data link layer connection is established (D-LINK_READY.indication(DLINKSTATUS=Link established), the EVCC shall initiate the IP address assignment mechanism as defined in subclauses 7.6.3.2 and 7.6.3.3.

ISO/DIS 15118-2:2018(E)
ISO/DIS 15118-2 ED2

- [V2G2-ED2-016]** The EVCC shall process the IP address assignment mechanism as defined in subclauses 7.6.3.2 and 7.6.3.3.
- [V2G2-ED2-017]** The EVCC shall stop the IP address assignment mechanism as defined in subclauses 7.6.3.2 and 7.6.3.3 when V2G_EVCC_CommunicationSetup_Timer is equal or larger than V2G_EVCC_CommunicationSetup_Timeout.
- [V2G2-ED2-018]** After a link-local IP address is assigned, the EVCC shall start the process for discovering the SECC address as defined in subclause 7.10.1.
- [V2G2-ED2-019]** The EVCC shall start the SDP client according to subclause 7.10.1.
- [V2G2-ED2-645]** Depending on the requested security and transport protocol in the SDP request message and the awaited security and transport protocol sent by SDP server, the EV shall decide on the application of TLS.
- [V2G2-ED2-020]** The EVCC shall stop the SDP when V2G_EVCC_CommunicationSetup_Timer is equal or larger than V2G_EVCC_CommunicationSetup_Timeout.
- [V2G2-ED2-021]** If the EV decides to apply a secured connection, the EVCC shall establish the TLS connection to the SECC as described in subclause 7.7.3 after the SECC IP address, port and available transport protocol and security options are discovered.
- [V2G2-ED2-646]** If the EV decides to apply an unsecured connection, the EVCC shall establish a TCP connection to the SECC as described in subclause 7.7.1 after the SECC IP address, port and available transport protocol and security options are discovered.
- [V2G2-ED2-022]** Depending on [V2G2-ED2-021] and [V2G2-ED2-646], the EVCC shall attempt to establish a TLS or TCP connection according to 7.7.3.
- [V2G2-ED2-023]** The EVCC shall stop to attempt to establish a TLS or TCP connection when V2G_EVCC_CommunicationSetup_Timer is equal or larger than V2G_EVCC_CommunicationSetup_Timeout.
- [V2G2-ED2-024]** After the TLS or TCP connection is established, the EVCC shall initiate the V2G communication session as defined in clause 8.
- [V2G2-ED2-025]** The EVCC shall terminate the TLS or TCP connection after stopping the V2G communication session.
- [V2G2-ED2-717]** If the EVCC sent the message SessionStopReq with parameter ChargingSession equal to "Terminate" it shall terminate the Data-Link (D-LINK_TERMINATE.request()) after receiving the message SessionStopRes.
- [V2G2-ED2-718]** If the EVCC sent the message SessionStopReq with parameter ChargingSession equal to "Pause" it shall pause the Data-Link (D-LINK_PAUSE.request()) after receiving the message SessionStopRes and continue with [V2G2-ED2-014].
- [V2G2-ED2-719]** Whenever the EVCC receives the indication for a missing Data-Link (D-LINK_READY.indication (DLINKSTATUS=No link), the EVCC shall continue with [V2G2-ED2-014].
- [V2G2-ED2-720]** If the EVCC identifies any error it shall indicate a Data-Link error (D-LINK_ERROR.request()) and continue with [V2G2-ED2-014].

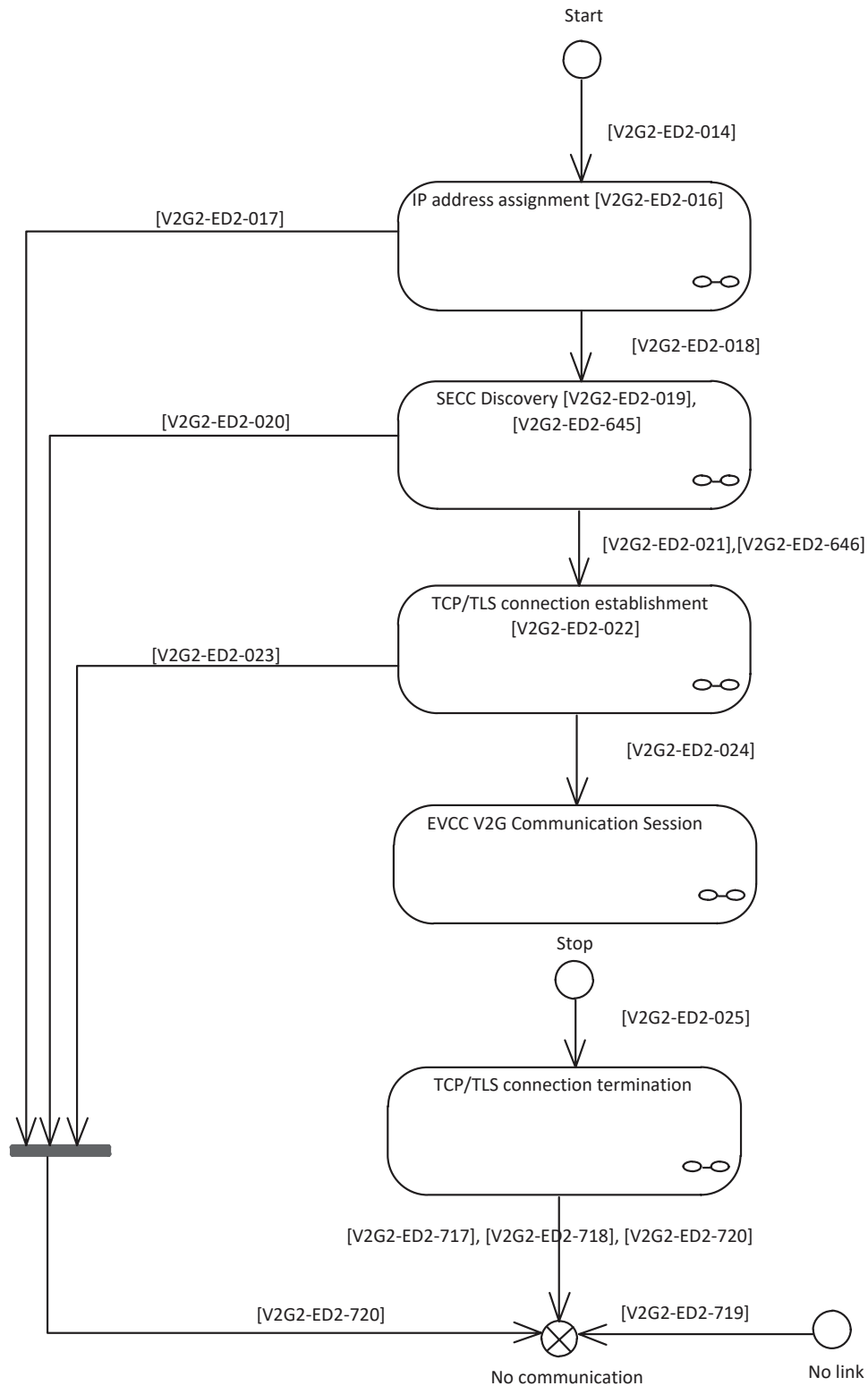


Figure 6 — Overview V2G communication states EVCC

Figure 7 depicts the general communication states of the V2G communication from an SECC perspective.

The following applies for the SECC:

ISO/DIS 15118-2:2018(E)
ISO/DIS 15118-2 ED2

- [V2G2-ED2-721]** After indication of a successful Data-Link establishment (D-LINK_READY.indication(DLINKSTATUS=Link established), the SECC shall initiate the address assignment mechanism.
- [V2G2-ED2-026]** The SECC shall configure an IP address (static or dynamic) by any appropriate mechanism.
- NOTE 1** To enable the integration of an SECC in different communication infrastructures, the definition of the address assignment for the SECC is out of scope of this standard. This enables the operator to assign an appropriate mechanism. E.g. the operator may choose any existing mechanism providing a valid IP address like e.g. a static IP or the mechanism described in subclauses 7.6.3.2 and 7.6.3.3.
- NOTE 2** The SECC shall be configured with a valid IP address for enabling a connection to an EVCC. The IP assignment mechanism for the SECC has no impact on compatibility and is not defined by this standard.
- [V2G2-ED2-027]** After the IP address is assigned, the SECC shall start the SDP server as defined in subclause 7.10.1.
- NOTE 3** It is not required that the SECC discovery service is implemented in the SECC directly. It is also possible to have a separate unit providing the SECC discovery service.
- [V2G2-ED2-723]** The SECC shall stop the SDP server when SECC_CommunicationSetup_Timer is equal or larger than V2G_SECC_CommunicationSetup_Performance_Time.
- [V2G2-ED2-029]** The SECC shall stop the IP address assignment mechanism when V2G_SECC_CommunicationSetup_Timer is equal or larger than V2G_SECC_CommunicationSetup_Performance_Time.
- [V2G2-ED2-030]** After the SDP server is started successfully, the SECC shall wait for a TLS or TCP connection initialization depending on the SDP response message as defined in subclause 7.10.1.5.
- [V2G2-ED2-031]** The SECC shall wait until the TLS or TCP connection is established.
- [V2G2-ED2-032]** The SECC shall stop waiting for establishing the TLS connection when V2G_SECC_CommunicationSetup_Timer is equal or larger than V2G_SECC_CommunicationSetup_Performance_Time.
- [V2G2-ED2-033]** After the TLS or TCP connection is established, the SECC shall wait for the initialization of the V2G communication session as defined in clause 8.
- [V2G2-ED2-722]** If [V2G2-ED2-033] applies the SECC can stop the SDP server after successful establishment of a TCP or TLS connection.
- [V2G2-ED2-034]** The SECC shall terminate the TLS or TCP connection after stopping the V2G communication session.
- [V2G2-ED2-724]** If the SECC received the message SessionStopReq with parameter ChargingSession equal to "Terminate" it shall terminate the Data-Link (D-LINK_TERMINATE.request()) after sending the message SessionStopRes.

- [V2G2-ED2-725]** If the SECC received the message SessionStopReq with parameter ChargingSession equal to "Pause" it shall pause the Data-Link (D-LINK_PAUSE.request()) after sending the message SessionStopRes and continue with [V2G2-ED2-721].
- [V2G2-ED2-726]** Whenever the SECC receives the indication for a missing Data-Link (D-LINK_READY.indication (DLINKSTATUS=No link), the SECC shall continue with [V2G2-ED2-721].
- [V2G2-ED2-727]** If the SECC identifies any error it shall indicate a data link error (D-LINK_ERROR.request()) and continue with [V2G2-ED2-721].

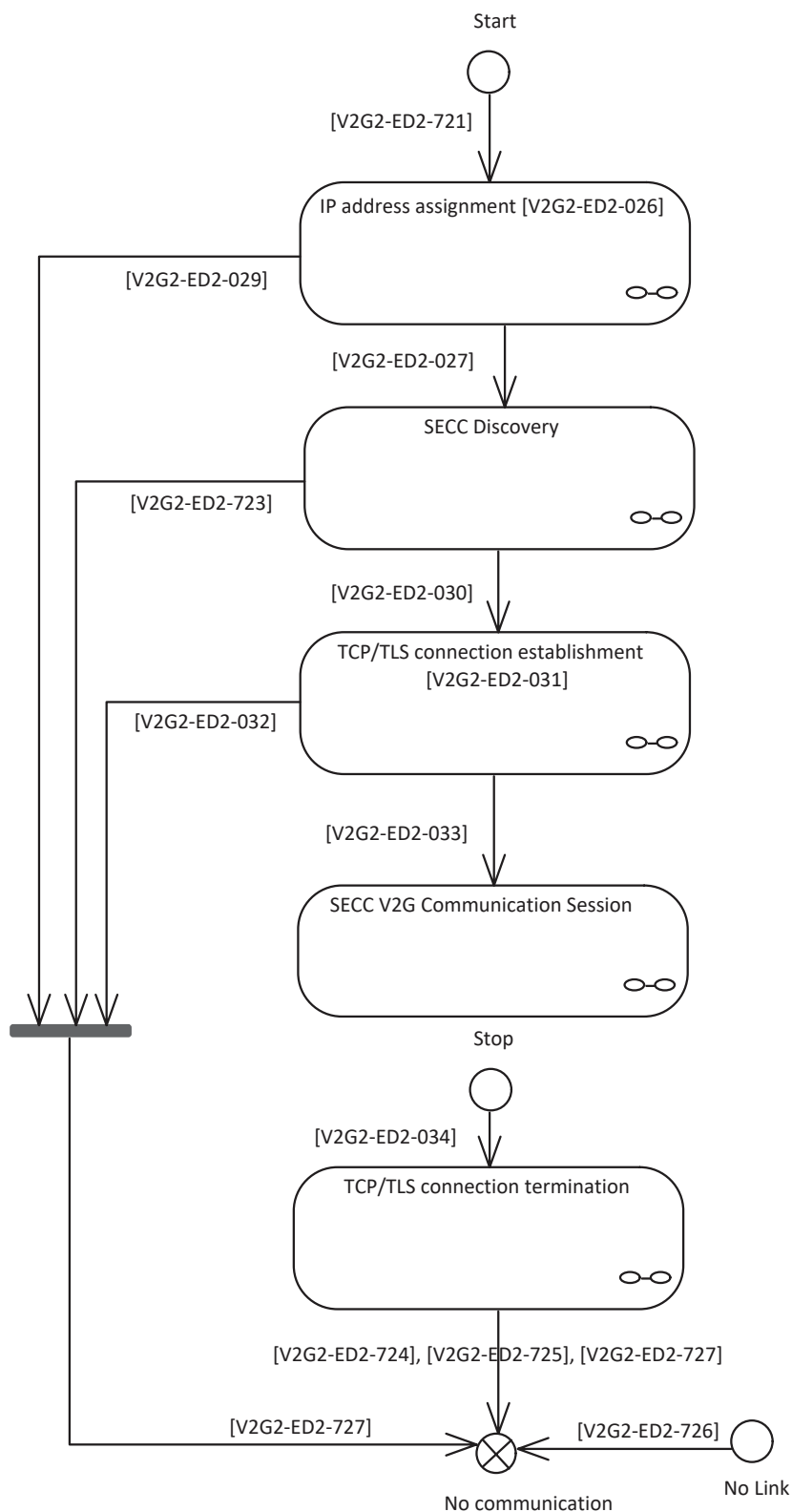


Figure 7 — Overview V2G communication session states SECC

7.5 Data link layer

The definitions in this document assume the Data Link layer to support the transport of IP packets as defined in the requirements. ISO 15118-3 and ISO 15118-8 define additional details on Data Link Layer to be covered.

[V2G2-ED2-035] If a V2G entity communicates by PLC, the V2G entity shall comply with ISO 15118-3.

[V2G2-ED2-1015] If a V2G entity communicates by Wireless LAN, the V2G entity shall comply with ISO 15118-8.

7.6 Network layer

7.6.1 General

The protocol specified in this standard is based on the Internet Protocol standard known as IPv6 (see IETF RFC 2460).

7.6.2 Applicable RFCs and limitations and protocol parameter settings

7.6.2.1 IPv6

[V2G2-ED2-037] A V2G Entity shall support IPv6 as defined in IETF RFC 2460.

[V2G2-ED2-1017] A V2G Entity shall fulfil the IPv6 node requirements specified in IETF RFC 4294.

[V2G2-ED2-038] While IETF RFC 2460 defines IPsec as mandatory, a V2G Entity is not required to implement IPsec.

[V2G2-ED2-039] No V2G Entity shall implement the RH0 routing header as specified IETF RFC 5095, which updates IETF RFC 2460.

NOTE The IANA allocation guidelines for the routing type field in the IPv6 routing header are described in IETF RFC 5871. It is recommended to adhere to these guidelines.

[V2G2-ED2-040] A V2G Entity shall implement path MTU discovery according to IETF RFC 1981.

[V2G2-ED2-041] A V2G Entity shall support handling of overlapping IP fragments according to IETF RFC 5722.

NOTE A V2G Entity should comply with the specification in IETF RFC 5220, which extends IETF RFC 2460.

[V2G2-ED2-042] When sending an IPv6 packet from EVCC to SECC or from SECC to EVCC no IP fragmentation shall be used.

NOTE The communication between EVCC and secondary actors is out of scope of this Part of ISO 15118 and may or may not use IP fragmentation.

[V2G2-ED2-1518] When sending an IPv6 packet containing charging related communication from EVCC to SECC or from SECC to EVCC the Traffic Class field in the IPv6 header shall be set to a value between 192 and 255.

[V2G2-ED2-1519] When sending an IPv6 packet containing non-charging related Value Added Service communication from EVCC to SECC or from SECC to EVCC the Traffic Class field in the IPv6 header shall be set to a value between 0 and 127.

7.6.2.2 Dynamic host control protocol (DHCPV6)

Data-link requirements are described in ISO 15118-3. The EVCC starts the address assignment triggered by the data-link when a data-link connection is established. This is done according to subclause 7.6.3.2 using SLAAC(Stateless auto address configuration), which is mandatory according to this standard. DHCPv6 might be implemented as an optional IP configuration method.

[V2G2-ED2-043] If an EVCC chooses to implement a DHCPv6 client, it shall implement it according to IETF RFC 3315.

[V2G2-ED2-1239] If the infrastructure the EV is connected to (EV supply equipment) chooses to implement a DHCPv6 server, it shall implement it according to IETF RFC 3315.

7.6.2.3 Neighbor discovery (ND)

The EVCC uses IPv6 SLAAC for generating addresses for its interface. All interfaces have a link-local address. To ensure unique addresses and to support global addresses the neighbour discovery protocol is used.

[V2G2-ED2-045] The EVCC shall implement neighborhood discovery as defined in IETF RFC 4861.

[V2G2-ED2-046] The EVCC shall comply with IETF RFC 4429 allowing assignment of IP addresses before Duplicate Address Detection is finished.

7.6.2.4 Internet control message protocol (ICMP)

The Internet Control Message Protocol (ICMP) is used to send error messages (e.g. a requested service is not available, a host could not be reached etc.).

[V2G2-ED2-047] Each V2G Entity shall implement ICMPv6 as specified in IETF RFC 4443.

[V2G2-ED2-049] Each V2G Entity shall implement the RFCs referred to in column 'Reference' of Table 5 describing the implementation details for the respective ICMP message type.

Table 5 — Mandatory ICMP message set

ICMP message type	ICMP message name	Reference
1	Destination Unreachable	IETF RFC 4443
2	Packet Too Big	IETF RFC 4443
3	Time Exceeded	IETF RFC 4443
4	Parameter Problem	IETF RFC 4443
128	Echo Request	IETF RFC 4443
129	Echo Reply	IETF RFC 4443
133	Router Solicitation	IETF RFC 4861
134	Router Advertisement	IETF RFC 4861
135	Neighbor Solicitation	IETF RFC 4861
136	Neighbor Advertisement	IETF RFC 4861
137	Redirect Message	IETF RFC 4861
141	Inverse Neighbor Discovery Solicitation Message	IETF RFC 3122
142	Inverse Neighbor Discovery Advertisement Message	IETF RFC 3122

7.6.3 IP addressing

7.6.3.1 General

This clause specifies how an EVCC retrieves valid IP addresses to communicate over an IP-based network. Following addresses are considered for the purpose of this standard:

- Link local IP address of EVCC
- Global IP address of EVCC, if router is present in local link
- IP address of SECC

NOTE An IPv6 host may have multiple IP addresses assigned to one physical network interface e.g. link-local and global address.

7.6.3.2 Stateless auto address configuration (SLAAC)

- [V2G2-ED2-050] Each V2G Entity shall support the configuration of a link-local IPv6 unicast address as specified in IETF RFC 4291.
- [V2G2-ED2-051] The interface ID of the Link-Local address of a V2G Entity shall be generated from its IEEE 48 bit MAC identifier according to the definition in IETF RFC 4291.
- [V2G2-ED2-052] The EVCC shall support auto configuration of IPv6 addresses as described in IETF RFC 4862.
- [V2G2-ED2-1520] If the SECC provides the Message Sets Certificate Install or Value Added Services as defined in subclause 8.6.4 it shall support IETF RFC 6106 for providing a DNS server address.

7.6.3.3 Address selection

- [V2G2-ED2-054] If multiple IPv6 addresses are supported, the IPv6 default address selection shall be performed according to IETF RFC 3484.

7.7 Transport layer

7.7.1 Transmission control protocol (TCP)

7.7.1.1 Overview

The transmission control protocol (TCP) allows applications of V2G Entities to establish a reliable data connection to other entities in order to exchange data in a reliable way and in-order. Additionally TCP provides flow control and congestion control and also provides for various algorithms to handle congestion and influence flow control.

7.7.1.2 Applicable RFCs, limitations and protocol parameter settings

- [V2G2-ED2-055] Each V2G Entity shall implement TCP as specified in IETF RFC 793.

7.7.1.3 TCP performance and checksum requirements

The following requirements define TCP implementation details relative to congestion control, retransmission, timing, initial window size and Selective Acknowledgement for the purpose of improving the overall performance of TCP.

It is recommended to use the following congestion control and retransmission algorithms in addition to the standard TCP methods:

ISO/DIS 15118-2:2018(E)
ISO/DIS 15118-2 ED2

- [V2G2-ED2-057]** Each V2G Entity should implement TCP congestion control according to IETF RFC 5681.
- [V2G2-ED2-059]** Each V2G Entity should compute TCP's retransmission timer according to IETF RFC 6298.
- [V2G2-ED2-060]** To increase TCP's performance each V2G Entity should implement TCP Extensions for High Performance according to IETF RFC 1323.
- [V2G2-ED2-062]** Each V2G Entity should implement the User Timeout Option according to IETF RFC 5482.
- [V2G2-ED2-063]** The urgent pointer for TCP shall not be used by any V2G Entity.

It is recommended to use the following checksum algorithm:

- [V2G2-ED2-064]** The checksum fields required in TCP headers should be implemented according to IETF RFC 1624.

7.7.2 User datagram protocol (UDP)

7.7.2.1 Overview

The User Datagram Protocol (UDP) is a connectionless protocol. UDP does not provide the reliability and ordering guarantees that TCP does. Packets may arrive out of order or may be lost without notification of the sender or receiver. However, UDP is faster and more efficient for many lightweight or time-sensitive purposes. UDP is located on the Transport Layer of the OSI layered architecture model.

Currently there is no use case utilizing UDP, for which security mechanisms on UDP would be required (refer ISO 15118-1 Annex L for details on security use cases).

7.7.2.2 Applicable RFC, limitations and protocol parameter settings

- [V2G2-ED2-065]** Each V2G Entity shall implement User Datagram Protocol according to IETF RFC 768.

7.7.3 Transport layer security (TLS)

7.7.3.1 Overview

Security on transport layer is being provided by using TLS. This allows to establish an authenticated and encrypted (ensures integrity protection and confidentiality protection) channel between the EVCC and the SECC. TLS allows for unilateral or mutual authentication. For ISO 15118 security it was agreed to use unilateral authentication (the EVCC authenticates the SECC).

7.7.3.2 Applicable RFCs

- [V2G2-ED2-067]** For the considered use cases unilateral authentication with TLS version 1.2 according to IETF RFC 5246 with extensions according to IETF RFC 6066 shall be supported by each V2G Entity. The EVCC authenticates the SECC by verifying the SECC Certificate (chain) provided from the SECC to the EVCC.
- [V2G2-ED2-1521]** TLS Versions higher than 1.2 may also be supported.

With unilateral authentication the EVCC authenticates the SECC according to [V2G2-ED2-067], which can also be used to protect the cyclic meter reading between the SECC and the EVCC. Application of unilaterally authenticated TLS saves the additional digital signature of meter readings on the SECC side due to the availability of a secure session.

NOTE In case of payment at the SECC, the cyclic meter reading is terminated at the SECC and does not need to be sent to a third party. Thus, there is no further signature of the billing relevant data necessary, contrary to the use cases ISO 15118-1 / C1 and C2 (contract credentials necessary), where billing relevant information is signed at application layer by the EVCC, if local regulations permit it, and forwarded through the SECC to the backend.

The application of unilateral authentication prohibits the SECC to verify the correctness of EVCC. Thus, the SECC may not detect, if the connecting EVCC is authentic. Verification of correctness of the EVCC can be achieved in the application layer as described subclause 7.9.2.

7.7.3.3 Transport layer security usage

[V2G2-ED2-068] The SECC shall always act as the TLS server component.

[V2G2-ED2-1240] "Each EVCC shall check the revocation status of the Sub-CA Certificates and the SECC leaf certificate (in the SECCs certificate chain) via an OCSF response according to IETF RFC 6960, when TLS is used. OCSF multi-stapling shall be used.

[V2G2-ED2-1522] The EVCC shall always support the signature_algorithm extension of TLS 1.2 (as defined in [RFC5246]) with the values {sha256, ecdsa}"

NOTE This prevents a fallback to {sha1, ecdsa} by the server if the signature algorithm extension is not send.

A "pairing mode" supports simple certificate management in private environments (see Annex N.2).

[V2G2-ED2-870] The EV can be set into a "pairing mode" using an OEM proprietary mechanism. This "pairing mode" shall only be activated by explicit user interaction. This mode shall automatically be reset after 120 seconds.

NOTE 2 The pairing mode can be re-activated any time.

NOTE 3 The OEM is suggested to explain the usage and the threats of the pairing mode e.g. in the user manual.

[V2G2-ED2-649] SECC should update (cache) the OCSF response at least once a week. One solution for updating might be for example an online connection.

[V2G2-ED2-876] The validity period of an OCSF response for a Sub-CA 1 and Sub-CA 2 shall be not longer than 4 weeks.

NOTE 4 This is aligned to the validity period of an SECC leaf certificate.

[V2G2-ED2-650] Although a valid time in the EVCC is not mandatory, the EVCC should implement a mechanism discarding outdated certificates from the SECC.

NOTE 5 It is out of scope of this standard how errors are handled. It is up to the OEM how these errors are handled.

[V2G2-ED2-651] The EVCC shall send a list of V2G root certificates it possesses, an extension of type "trusted_ca_keys" in the (extended) client hello as defined in IETF RFC 6066. The "cert_sha1_hash" that contains the SHA-1 hash of a DER-encoded Certificate containing the CA root key shall be used as a unique CA root key identifier.

[V2G2-ED2-871] If an SECC is deployed in an environment that is not a private environment, it shall send its own certificate and a chain up to a root (excluding the root certificate itself) which shall be one of those roots previously indicated by the EVCC as being present in the EVCC. If the EVCC has requested OCSF responses, for each certificate that the TLS server responds with, an OCSF response shall be sent to EVCC, as defined in IETF RFC 6961. The OCSF

responder shall fill the field “certs” in the OCSP response (BasicOCSPResponse) structure according to IETF RFC 6960 sec 4.2.1. The SECC shall also send the certificate of the OCSP responder if it is not the corresponding Sub-CA itself.

NOTE 6 As defined in IETF RFC2560, an OCSP responder might either be the Sub-CA itself, or it might be an entity which is directly signed by the corresponding Sub-CA using a key pair with a special extended key usage flag in the certificate.

[V2G2-ED2-923] If the SECC cannot provide a certificate with a chain up to one of the roots which the EVCC signaled as being present in EVCC, the SECC shall provide within the TLS handshake a valid certificate including a chain to a root certificate (The root certificate itself shall not be transmitted).

[V2G2-ED2-924] If the SECC has provided a certificate chain that does not trace up to a root certificate in the list of trusted certificates, the EVCC shall only accept such a certificate, if it successfully validated the certificate chain using an out of band validation mechanism (e.g. server based certificate validation protocol, SCVP, according to RFC 5055). If the validation using such a service is not done, gives a negative result or fails (e.g. due to missing connectivity), the EVCC shall treat the certificate chain as not validated.

[V2G2-ED2-872] If an SECC is deployed in a private environment, the SECC shall not send an OCSP response, but the SECC shall include its own private root certificate in the certificate chain it sends.

NOTE 7 This supports the “pairing mode”

[V2G2-ED2-873] In case the EVCC previously required an OCSP response via TLS “client hello”, and the TLS server has not sent OCSP responses in “server hello”, the EVCC shall do the following:

- If the TLS server certificate chain contains only one leaf certificate and one root certificate, which is one of the root certificates that the EV has stored as a private root, the EV ignores the fact, that the server has not sent OCSP responses.
- If the TLS server certificate chain is linked to a V2G root, the EVCC shall abort the TLS connection.

[V2G2-ED2-874] If the pairing mode is currently activated, the EVCC receives a new root certificate from the SECC during TLS handshake, and the new root certificate fulfills the requirements for private root certificates (see [Certificate Profiles]), then the EVCC shall accept the new root certificate, store it permanently, and treat it as a private root certificate.

[V2G2-ED2-875] The EVCC shall verify the SECC Certificate, the complete certificate chain and all OCSP responses (if applicable, including the validity of OCSP responder). The EVCC shall also verify that the SECC Certificate has the Domain Component set to “CPO”. If at least one of these verifications fails, the EVCC shall abort the TLS setup process and apply [V2G2-ED2-023].

[V2G2-ED2-810] The SECC shall support Maximum Fragment Length Negotiation according to IETF RFC 6066.

[V2G2-ED2-811] The SECC shall be able to support, but not be limited to a maximum fragment length of 2⁹ bytes according to IETF RFC 6066.