



DPC: 25/30509159 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 26 August 2025

Origin: European

Latest date for receipt of comments: 19 October 2025

Project No. 2025/00297

Responsible committee: PEL/69 Electric vehicles

Interested committees:

Title: Draft BS EN ISO 15118-2 Road vehicles — Vehicle-to-Grid Communication Interface. Part 2: Network and application protocol requirements.

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

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

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 19 October 2025

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

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

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

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

Responsible Committee Secretary: Ms Andreea Vieru (BSI)

Direct tel: 0208 996 7432

E-mail: andreea.vieru@bsigroup.com

Full document details: 25/30509159 DC

Introduction

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

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

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

UK Vote

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

Submission of Comments

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

Template for comments and secretariat observations

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

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



DRAFT International Standard

ISO/DIS 15118-2

Road vehicles — Vehicle-to-Grid Communication Interface —

Part 2: Network and application protocol requirements

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

Partie 2: Exigences du protocole d'application et du réseau

ICS: 43.120

ISO/TC 22/SC 31

Secretariat: **DIN**

Voting begins on:
2025-08-26

Voting terminates on:
2025-11-18

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 15118-2:2025(en)

Full document details: 25/30509159 DC

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

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

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

© ISO 2025



Documents

Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO 2025

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

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

Published in Switzerland

Contents

Foreword.....	vii
Introduction.....	ix
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions.....	3
4 Abbreviated terms.....	7
5 Conventions.....	8
5.1 Definition of OSI based services.....	8
5.2 Requirement structure.....	8
5.3 Usage of RFC references.....	9
5.4 Notation used for XML schema diagrams.....	9
6 Document overview.....	9
7 Basic requirements for V2G communication.....	11
7.1 General information.....	11
7.2 Service primitive concept of OSI layered architecture.....	11
7.2.1 Overview.....	11
7.2.2 Syntax of service primitives.....	12
7.3 Security concept.....	12
7.3.1 Call flows (flow charts).....	12
7.3.2 Certificate and key management.....	16
7.3.3 Number of root certificates and root validity, certificate depth and size.....	18
7.3.4 Support and application of TLS.....	19
7.4 V2G communication states and data link handling.....	21
7.5 Data link layer.....	26
7.6 Network layer.....	26
7.6.1 General.....	26
7.6.2 Applicable RFCs and limitations and protocol parameter settings.....	26
7.6.3 IP addressing.....	27
7.7 Transport layer.....	28
7.7.1 Transmission control protocol (TCP).....	28
7.7.2 User datagram protocol (UDP).....	29
7.7.3 Transport layer security (TLS).....	29
7.8 V2G transfer protocol.....	32
7.8.1 General.....	32
7.8.2 Supported ports.....	33
7.8.3 Protocol data unit.....	34
7.9 Presentation layer.....	37
7.9.1 XML and efficient XML interchange (EXI).....	37
7.9.2 Message security.....	40
7.10 Application layer.....	47
7.10.1 SECC discovery protocol.....	47
7.10.2 Vehicle to grid application layer messages.....	52
7.10.3 Application layer service primitives.....	52
8 Application layer messages.....	56
8.1 General.....	56
8.2 Protocol handshake definition.....	57
8.2.1 Handshake sequence.....	57

8.2.2	Message definition supportedAppProtocolReq and supportedAppProtocolRes	58
8.2.3	Semantics description supportedAppProtocol messages.....	59
8.2.4	Message examples.....	60
8.3	V2G message definition.....	61
8.3.1	General.....	61
8.3.2	Message definition.....	61
8.3.3	Message header definition.....	62
8.3.4	Message body definition	63
8.4	V2G communication session and BodyElement definitions	64
8.4.1	General.....	64
8.4.2	Session handling.....	65
8.4.3	Common messages.....	68
8.4.4	AC messages	99
8.4.5	DC messages.....	102
8.5	Complex data types.....	111
8.5.1	Overview	111
8.5.2	Common.....	111
8.5.3	AC	140
8.5.4	DC.....	144
8.6	Identification modes and message set definitions	152
8.6.1	Overview	152
8.6.2	Supported message sets.....	154
8.6.3	Selection of message sets	180
8.7	V2G communication timing	185
8.7.1	Overview	185
8.7.2	Message sequence and communication session	186
8.7.3	Session setup and ready to charge.....	191
8.7.4	V2G message synchronization with IEC 61851-1 signalling.....	200
8.8	Message sequencing and error handling.....	220
8.8.1	Overview	220
8.8.2	Basic Definitions for Error Handling.....	221
8.8.3	ResponseCode handling.....	222
8.8.4	Request-response message sequence requirements.....	227
8.9	Request-response message sequence examples.....	276
8.9.1	AC	276
8.9.2	DC.....	279
	Annex A (normative) Schema definition.....	286
A.1	Overview.....	286
A.2	V2G_CI_AppProtocol.xsd	287
A.3	V2G_CI_MsgDef.xsd.....	287
A.4	V2G_CI_MsgHeader.xsd.....	288
A.5	V2G_CI_MsgBody.xsd	288
A.6	V2G_CI_MsgDataTypes.xsd	296
A.7	xmldsig-core-schema.xsd	305
	Annex B (normative) Certificate profiles.....	310
	Annex C (normative) Specification of identifiers.....	318
C.1	e-Mobility authentication identifier (EMAID).....	318
C.1.1	EMAID syntax.....	318

C.1.2	EMAID Semantics	318
C.1.3	Calculation of the check digit	319
C.2	Electric vehicle supply equipment ID (EVSEID).....	319
C.2.1	EVSEID syntax	319
C.2.2	EVSEID semantics	320
Annex D (informative)	Mapping of ISO 15118-1 use case elements	321
D.1	Relation of identification modes and use case elements.....	321
Annex E (informative)	Message examples	376
E.1	Value added service selection	376
E.2	EXI encoded message examples.....	378
E.2.1	SessionSetupRes message	378
E.2.2	ChargeParameterDiscoveryReq message (AC-based).....	379
E.2.3	CurrentDemandReq message.....	379
E.3	Schedules and tariff information	380
E.3.1	Overview	380
E.3.2	Dynamic GridSchedule w/o SalesTariff over ISO 15118 V2G CI	380
E.3.3	“Time Of Use”-based SalesTariff with constant value for GridSchedule.....	382
E.3.4	“Time Of Use”-based SalesTariff with dynamic GridSchedule.....	383
E.3.5	“Consumption”-based SalesTariff with constant value for GridSchedule	385
E.3.6	Multiple SalesTariffs with different demand Limits in GridSchedule	386
E.3.7	Time of Use-based SalesTariffs including relativePricePercentage	388
Annex F (informative)	Application of certificates.....	397
F.1	General information	397
F.1.1	Overview	397
F.1.2	Demands of the OEM.....	398
F.1.3	Demands of the secondary actors.....	398
F.1.4	Rationale for decisions in this document	399
F.1.5	Overview of the resulting certificate structure	401
F.2	Simplified certificate management in private environment.....	402
F.2.1	Overview (motivation)	402
F.2.2	Solution for private environments.....	402
F.2.2.1	General	402
F.2.2.2	Installation of a private root certificate into a vehicle.....	403
F.2.2.3	Charging in a private environment	403
F.2.2.4	Compromised certificate of a wall box.....	403
F.3	Use of OEM provisioning certificates	404
F.3.1	Introduction	404

F.3.2 Processes.....405

F.3.2.1 Vehicle production 405

F.3.2.2 Vehicle Hand-Over 406

F.3.2.3 Contract Conclusion 406

F.3.2.4 Certificate installation.....406

F.3.2.5 Certificate update.....406

F.3.2.6 Component replacement 406

F.4 Security appliances and their associated certificates 407

Annex G (informative) Encryption for the distribution of secret keys 410

G.1 Overview.....410

G.2 Ephemeral-static Diffie-Hellman key agreement 410

G.3 Key pairs.....411

Annex H (informative) Message sequencing for renegotiation 412

H.1 Overview.....412

Annex I (informative) Overview on XML signatures 419

I.1 Overview.....419

I.2 Signature generation.....419

I.3 Signature generation for secondary actors.....422

I.4 Signature validation 422

Annex J (informative) Summary of requirements.....424

Annex K (informative) Use of Multiple Contracts in ISO 15118-2 432

Bibliography.....434

Foreword

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

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

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

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

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

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

The main changes are as follows:

- General corrections identified and resolved by the “ISO 15118-2 User Group” (most, if not all, of these corrections are already included in existing implementations in the field, since the underlying issues were identified during various Test Symposia);
- Clarification how to properly use the ChargingProfile;
- Clarification of the interaction between ISO 15118-2 and IEC 61851 during the charging sequence;
- Introduction of a means to activate an ad-hoc charge control with EIM and PnC;
- Clarification of error handling and shutdown scenarios;
- Introduction of a means to stop the V2G communication session before the V2G charge loop (external trigger by the user or the charging application);
- Clarification how to use multiple Contract Certificates;
- Removal of the definition of certificate lifetimes, because they should be defined by PKI;
- Removal of the general obligation to use TLS with value added services, because whether or not TLS must be used should be mandated by the specification of the respective value added service;
- Alignment of TCP behaviour (timeouts, retries, ...) with ISO 15118-20.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The pending energy crisis and necessity to reduce greenhouse gas emissions has led the vehicle manufacturers to a very significant effort to reduce the energy consumption of their vehicles. They are presently developing vehicles partly or completely propelled by electric energy. 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 the batteries of such vehicles, specific charging infra-structure is required.

Much of the standardization work on dimensional and electrical specifications of the charging infrastructure and the vehicle interface is already treated in the relevant ISO or IEC groups. However, the question of information transfer between the EV and the EVSE has not been treated sufficiently.

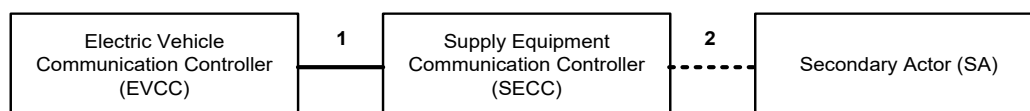
Such communication is necessary for the optimization of energy resources and energy production systems so that vehicles can recharge in the most economical or most energy efficient way. It is also required to develop efficient and convenient billing systems to cover the resulting micro-payments. The necessary communication channel may serve in the future to contribute to the stabilization of the electrical grid as well as to support additional information services required to operate electric vehicles efficiently and economically.

Road vehicles — Vehicle-to-grid communication interface — Part 2: Network and application protocol requirements

1 Scope

This document specifies the communication between battery electric vehicles (BEV) or plug-in hybrid electric vehicles (PHEV) and the Electric Vehicle Supply Equipment. The application layer message set defined in this document is designed to support the energy transfer from an EVSE to an EV. ISO 15118-1 contains additional use case elements (Use Case Element IDs: F4 and F5) describing the bidirectional energy transfer. The implementation of these use cases requires enhancements of the application layer message set defined herein.

The purpose of this document is to detail the communication between an EV (BEV or a PHEV) and an EVSE. 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 In scope of this document
- 2 Message definition considers use cases defined for communication between SECC to SA

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

This document defines messages, data model, XML/EXI based data representation format, usage of V2GTP, TLS, TCP and IPv6. In addition, it describes 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 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*

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

IEC 61851-23, *Electric vehicle conductive charging system - Part 23: D.C. electric vehicle charging station*

IEC 62196-2, *Plugs, socket-outlets, vehicle connectors and vehicle inlets – Conductive charging of electric vehicles – Part 2: Dimensional compatibility and interchangeability requirements for A.C. pin and contact-tube accessories*

IEC 62196-3, *Plugs, socket-outlets, vehicle connectors and vehicle inlets – Conductive charging of electric vehicles – Part 3: Dimensional compatibility and interchangeability requirements for DC and AC/DC pin and contact-tube vehicle couplers*

W3C EXI 1.0, *Efficient XML Interchange (EXI) Format 1.0, W3C Recommendation*

IETF RFC 768, *User Datagram Protocol*

IETF RFC 793, *Transmission Control Protocol - DARPA Internet Program - Protocol Specification*

IETF RFC 1630, *Universal Resource Identifiers in WWW*

IETF RFC 1981, *Path MTU Discovery for IP version 6*

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

IETF RFC 6960:2013, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*

IETF RFC 3122, *Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification*

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

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

IETF RFC 4291, *IP Version 6 Addressing Architecture*

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

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

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

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

IETF RFC 4862, *IPv6 Stateless Address Autoconfiguration*

IETF RFC 5095, *Deprecation of Type 0 Routing Headers in IPv6*

IETF RFC 5234, *Augmented BNF for Syntax Specifications: ABNF*

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

IETF RFC 5289, *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*

IETF RFC 5480, *Elliptic Curve Cryptography Subject Public Key Information*

IETF RFC 5722, *Handling of Overlapping IPv6 Fragments*

IETF RFC 6066, *Transport Layer Security (TLS) Extensions: Extension Definitions*

IETF RFC 6106, *IPv6 Router Advertisement Options for DNS Configuration*

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

W3C EXI Profile, *Efficient XML Interchange (EXI) Profile, W3C Candidate Recommendation*

IANA Service&PortRegistry, *Service Name and Transport Protocol Port Number Registry*¹

NIST FIPS PUB 180-4, *Secure Hash Standard (SHS)*

NIST Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*

NIST Special Publication 800-38A, *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*

¹ Available from: <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml>

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 15118-1 and the following 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 <http://www.electropedia.org/>

3.1

ad-hoc charging

mode of *HLC-C* where no power schedule but only one upper power limit is requested by the EVCC and/or provided by the SECC before *HLC-C*, and where a *renegotiation* of the charging limits is prohibited, and where, any time during the *V2G charging loop*, the SECC is allowed to reduce ad-hoc its upper power and/or current limit to a (corresponding) value below the initially provided upper power limit

3.2

basic charging

BC

energy transfer phase during an AC charging session that is only controlled by *control pilot states* according to IEC 61851-1 (Annex A)

3.3

charging

energy transfer, where the direction is restricted to energy transfer from the EVSE to the EV

Note 1 to entry: In this document the term "charging" is used synonymously to the term "energy transfer".

3.4

charging limit

physical constraint (e.g. voltage, current, energy, power) that is negotiated during a *V2G Communication Session* (3.36) for a charging session

3.5

contract certificate

certificate issued to EVCC either by *V2G root CA* (3.42) or by *Sub-CA* (3.29), 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

3.6

control pilot state

CP state

system state according to IEC 61851-1 (Annex A) signalled on control pilot line

3.7

credentials

anything that provides the basis for confidence, belief, credit, etc.

EXAMPLE Certificates, passwords, user names, etc..

3.8

data link setup

setup phase for establishing the data link

Note 1 to entry: Entry condition: Any valid control pilot signal according to IEC 61851-1 and ISO 15118-3 (i.e. a CP state BX or CX or DX, where $X = 1$ or 2); Exit Condition: D-LINK_READY.indication(DLINKSTATUS=LinkEstablished).

3.9**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

3.10**global address**

IP address with unlimited scope

3.11**high level communication charging****HLC-C**

energy transfer phase during a charging session controlled by parameters (e.g. charging limits) that are communicated via digital communication as specified in this document, in addition to the charge control by *control pilot states* according to IEC 61851-1 (Annex A)

3.12**link-local address**

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

3.13**identification mode**

mandatory and optional messages and parameters with respect to charging scenarios using external identification means (EIM) and charging scenarios using plug and charge (PnC) for identification

Note 1 to entry: An identification mode covers a set of similar charging scenarios for a specific identification means.

3.14**IP address**

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

3.15**maximum transfer unit****MTU**

size of the largest protocol data unit (in bytes) that can be communicated in a single network layer transaction

3.16**message set**

set of mandatory *V2G messages* (3.38) and parameters for the EVCC or SECC covering one or multiple use case elements

3.17**message timer**

timer monitoring the exchange of a *request-response-message-pair* (3.23)

3.18**OEM provisioning certificate**

certificate issued to the EVCC, so that a *contract certificate* (3.3) can be securely requested and received from a secondary actor

3.19**performance time**

non-functional timing requirement defining the time a *V2G entity* (3.37) shall not exceed when executing or processing certain functionality

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

3.20**private environment**

environment which is not using certificates derived from a V2G root, but certificates that are derived from a private root certificate, which is only distributed to a limited number of EV

Note 1 to entry: In a private environment, the EVSE can stay offline permanently.

Note 2 to entry: The permanent offline operation simplifies certificate handling for the EVSE through unrestricted certificate validity periods (in particular, a longer maximum validity of the leaf certificates than allowed for public charging stations), shorter certificate chain length (using a private root certificate in the EVs that are admitted to a specific private environment), omitting OCSP, and omitting an additional “pairing mode”.

Note 3 to entry: TLS is always used in a private environment.

EXAMPLE 1 A private parking garage.

EXAMPLE 2 A garage/ parking lot of a company with its own EV fleet, where one or several private wall-box(es) are used instead of public charging stations as EVSE.

3.21**renegotiation**

messaging for updating the agreement on the charging schedule between EV and EVSE during a *V2G communication session* (3.36) by retransmitting the parameters *SASchedule* and *ChargingProfile*

3.22**request-response message pair**

request message and the corresponding response message

3.23**request-response message sequence**

predefined sequence of *request-response message pairs* (3.23)

3.24**scheduled charging**

mode of *HLC-C* where a power schedule with more than one upper power limit and optionally a tariff table, both with a certain duration, are negotiated between the EVCC and the SECC before *HLC-C*, and where the SECC will try its best to provide the reserved upper power limits during the *V2G charging loop*, and where a *renegotiation* of the power schedule is allowed

3.25**SDP client**

V2G entity (3.37) that uses the *SDP server* (3.26) to get configuration information about the SECC to be able to access the SECC

3.26**SDP server**

V2G entity (3.37) providing configuration information for accessing the SECC

3.27**SECC certificate**

certificate issued to SECC either by *V2G root CA* (3.42) or by *Sub-CA* (3.29), which is used in TLS so that the EVCC can verify the authenticity of the SECC

3.28**sequence timer**

timer monitoring a *request-response message sequence* (3.24)

3.29**sub-CA**

subordinate certificate authority that issues *SECC certificates* (3.27) and/or *contract certificates* (3.3) on behalf of the *V2G root CA* (3.42)

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.

3.30**sub-CA certificate**

certificate issued to *sub-CA* (3.29)

3.31**TCP_DATA**

socket/interface for data transfer based on TCP connection

3.32**timeout**

timing requirement defining the time a *V2G entity* (3.37) monitors the communication system for a certain event to occur

Note 1 to entry: If the specified time is exceeded the respective *V2G entity* (3.37) initiates the related error handling. This is a fixed time value.

3.33**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.

3.34**trusted environment**

closed user group with some pre-distributed token for access to the SECC charging service (e.g. key to home garage, RFID token for car sharing), which is something where a person or instance is responsible for

EXAMPLE A person with its home garage, a car sharing operator or a taxi operator.

3.35**V2G charging loop**

V2G messaging phase for controlling the charging process

3.36**V2G communication session**

association of two specific *V2G entities* (3.37) for exchanging V2G messages

3.37**V2G entity**

primary actor participating in the V2G communication using a mandatory or optional transmission protocol

3.38**V2G message**

message exchanged on application layer

Note 1 to entry: Refer to Clause 8.

3.39**V2G setup**

setup phase for V2G messaging

Note 1 to entry: Entry condition: D-LINK_READY.indication(DLINKSTATUS=LinkEstablished); exit condition: PowerDeliveryReq with ChargeProgress equals start or stop.

3.40

V2G transfer protocol

communication protocol to transfer *V2G messages* (3.38) between two V2GTP entities

3.41

V2GTP entity

V2G entity (3.37) supporting the *V2G transfer protocol* (3.40)

3.42

V2G root CA

certificate authority (CA) that issues *contract certificates* (3.3) and/or *SECC certificates* (3.27), or that delegates ability to issue such certificates to *sub-CA* (3.29)

3.43

V2G root certificate

certificate issued to *V2G root CA* (3.42)

4 Abbreviated terms

BEV	battery electric vehicle
CA	certificate authority
CRL	certificate revocation list
DH	Diffie Hellman
DER	distinguished encoding rules
ECDSA	elliptic curve digital signature algorithm
EMAID	E-mobility account identifier
EMSP	E-Mobility Service Provider
EV	electric vehicle
EVCC	electric vehicle communication controller
EVSE	electric vehicle supply equipment
EXI	efficient XML interchange
OCSP	online certificate status protocol
OEM	original equipment manufacturer
PDU	protocol data unit
PHEV	plug-in hybrid electric vehicle
PKI	public key infrastructure
PLC	power line communication
PnC	plug and charge
SA	secondary actor
SDP	SECC discovery protocol
SDU	service data unit
SECC	supply equipment communication controller

SLAAC	stateless auto address configuration
TCP	transmission control protocol
VAS	value added service
V2G	vehicle-to-grid communication
V2G CI	vehicle-to-grid communication interface
V2GTP	V2G transfer protocol
UDP	user datagram protocol
XML	extensible markup language

5 Conventions

5.1 Definition of OSI based services

This document is based on the conventions discussed 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 newly added and updated requirements:

"[V2G2-"XXXX"]" requirement text, where:

- "V2G2" represents this document,
- "XXXX" represents the unique requirement number consisting of four digits starting from 1 000, and
- "requirement text" includes the actual text of the requirement.
- For purely AC or DC specific requirements, an identifier is added as follows: "[V2G2-"XXXX"] [AC]" or "[V2G2-"XXXX"] [DC]", respectively

NOTE 1 If technical changes have been done to requirements of ISO 15118-2 Ed.1, their requirement number has been updated to above format.

EXAMPLE 1 [V2G2-0000] This shall be an example requirement introduced in this document.

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

"[V2G2-"YYY"]" requirement text, where:

- "V2G2" represents this document,
- "YYY" represents the unique requirement number as already defined in ISO 15118-2 Ed.1, and
- "requirement text" is the same text as specified in ISO 15118-2 Ed.1.

NOTE 2 If editorial changes have been done to requirements of ISO 15118-2 Ed.1, their requirement number has not been changed.

EXAMPLE 2 [V2G2-000] This shall be an example requirement originally defined in ISO 15118-2 Ed.1.

5.3 Usage of RFC references

When RFCs are referenced all “shall/shall not” requirements are mandatory.

[V2G2-1026] In this document, if a referenced RFC has been updated by one or several RFC, the update shall be fully applicable.

[V2G2-002] If an update or part of an update applicable to an RFC referenced herein is not compatible with the original RFC or the implementation described by this document the update shall not apply.

[V2G2-1027] If there are erratas published for any RFCs referenced in this document, they shall be applicable.

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 Altova XMLSpy Manual.

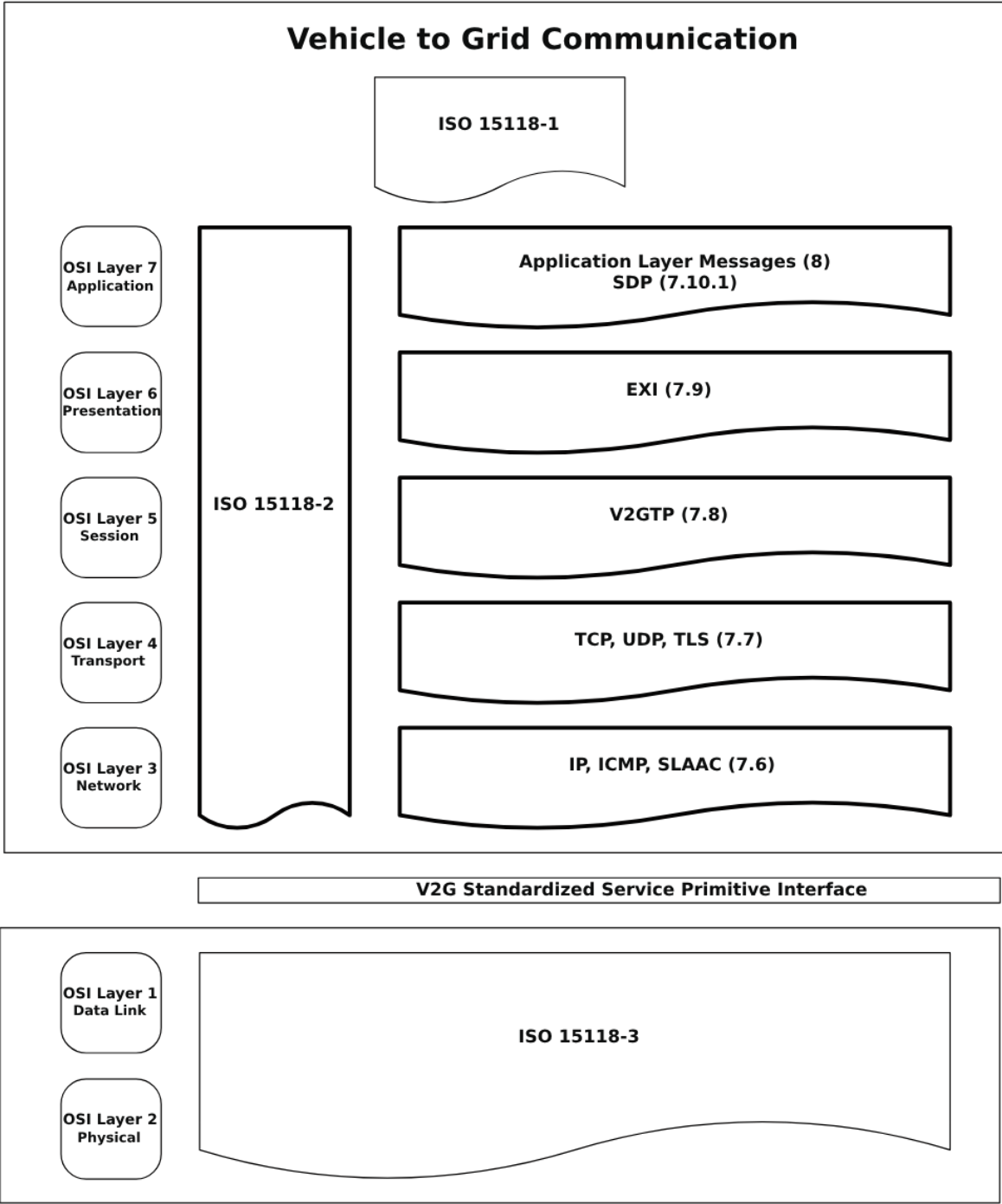
Allowing for an easy way to distinguish the types used for the XML schema definitions in this document following naming conventions apply:

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

6 Document overview

Figure 2 describes the organization of the 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 2 requirements including the V2G standardized service primitive interface are specified in ISO 15118-3.



Key

- OSI Layers and applicable requirements described in this document
- OSI Layers and applicable requirements defined in other parts of the ISO 15118 series

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 cases elements defined in ISO 15118-1.

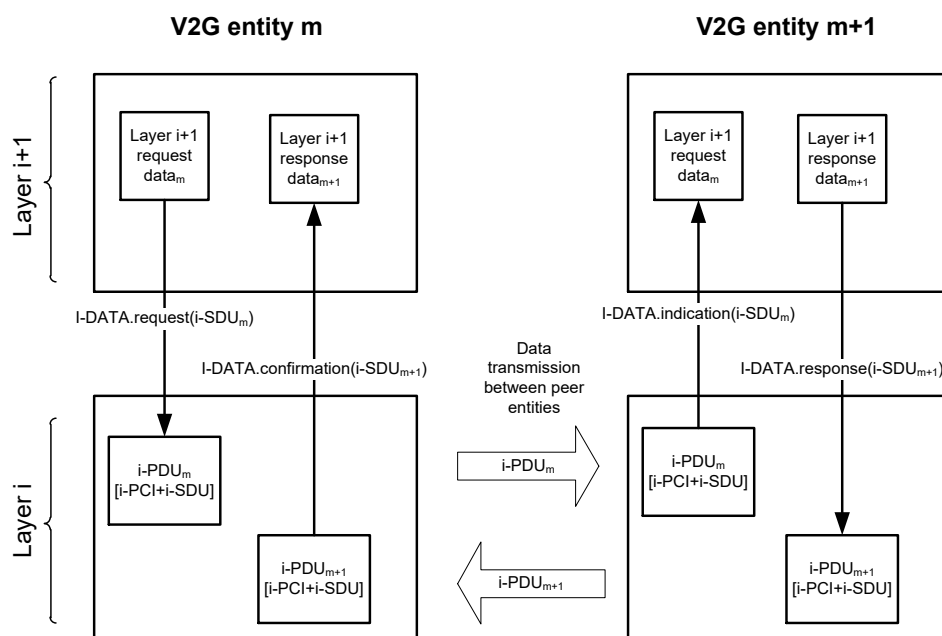
7.2 Service primitive concept of OSI layered architecture

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

PDUX: Protocol Data Unit of network entity x

PCI: Protocol Control Information

SDUx: 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)

- 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 document 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 Call flows (flow charts)

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 8.8. In these overview figures (Figure 4 and Figure 5) only the security relevant information shall be highlighted.

The security concept provides a basic transport-based protection mechanism. For certain scenarios, the usage of transport layer security (TLS) for the transport communication between EVCC and SECC is mandated. For some other scenarios, the usage of TLS is optional. Specific messages are protected on application layer (XML-messages), if data are protected on the way from or to a secondary actor, or if the protection lasts longer than the existence of the TLS channel. Also the concept is independent from any further protection mechanisms on lower levels than layer 3 in the OSI layer model.

Figure 4 shows an example use case for a semi-online connection for a plug and charge scenario:

In this plug and charge example, all TCP/IP based communication is protected using a unilaterally authenticated TLS channel between the two peers. (TLS is not mandatory for certain identification modes other than the plug and charge identification mode.) 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 EVSE provides the charging records, containing 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 purposes only and not intended to specify a particular message sequence.

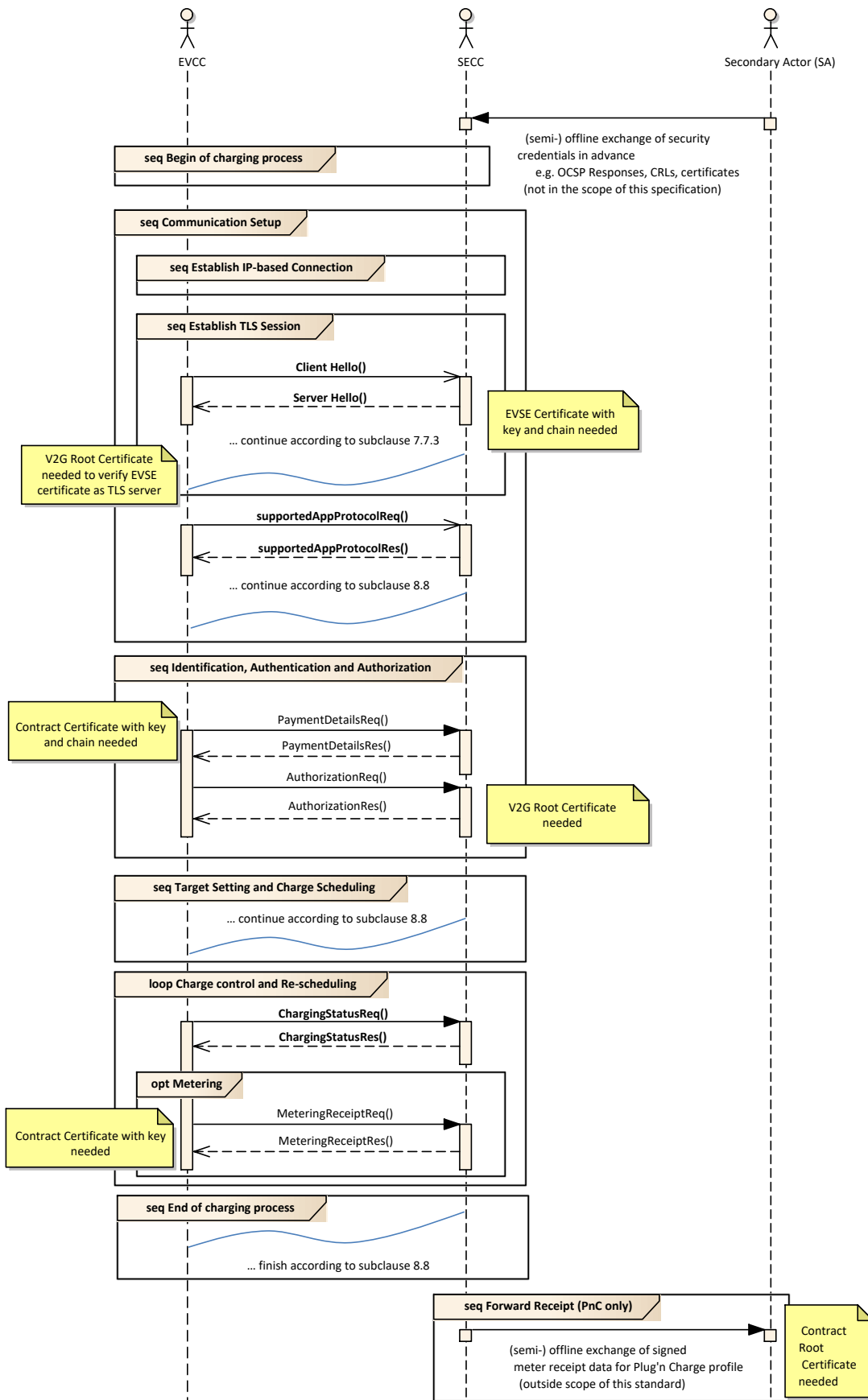


Figure 4 — Example for semi-online communication

Figure 5 shows an example for an online plug and charge use case:

As in the semi-online case, in this plug and charge example, all TCP/IP based communication is protected using a unilaterally authenticated TLS channel between the two peers.

NOTE 2 TLS is not mandatory for certain identification modes other than the plug and charge identification mode.

Some of the information provided by the vehicle may need to be sent to the SA for further processing, like the eMAID or the vehicles credentials to be able to sign the tariff information. The EVCC calculates a charging profile (refer to 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, although the security of the vehicle communication to the SA is secured on application layer.

NOTE 3 The communication between SECC and SA in Figure 5 is shown for informational purposes only and not intended to specify a particular message sequence.

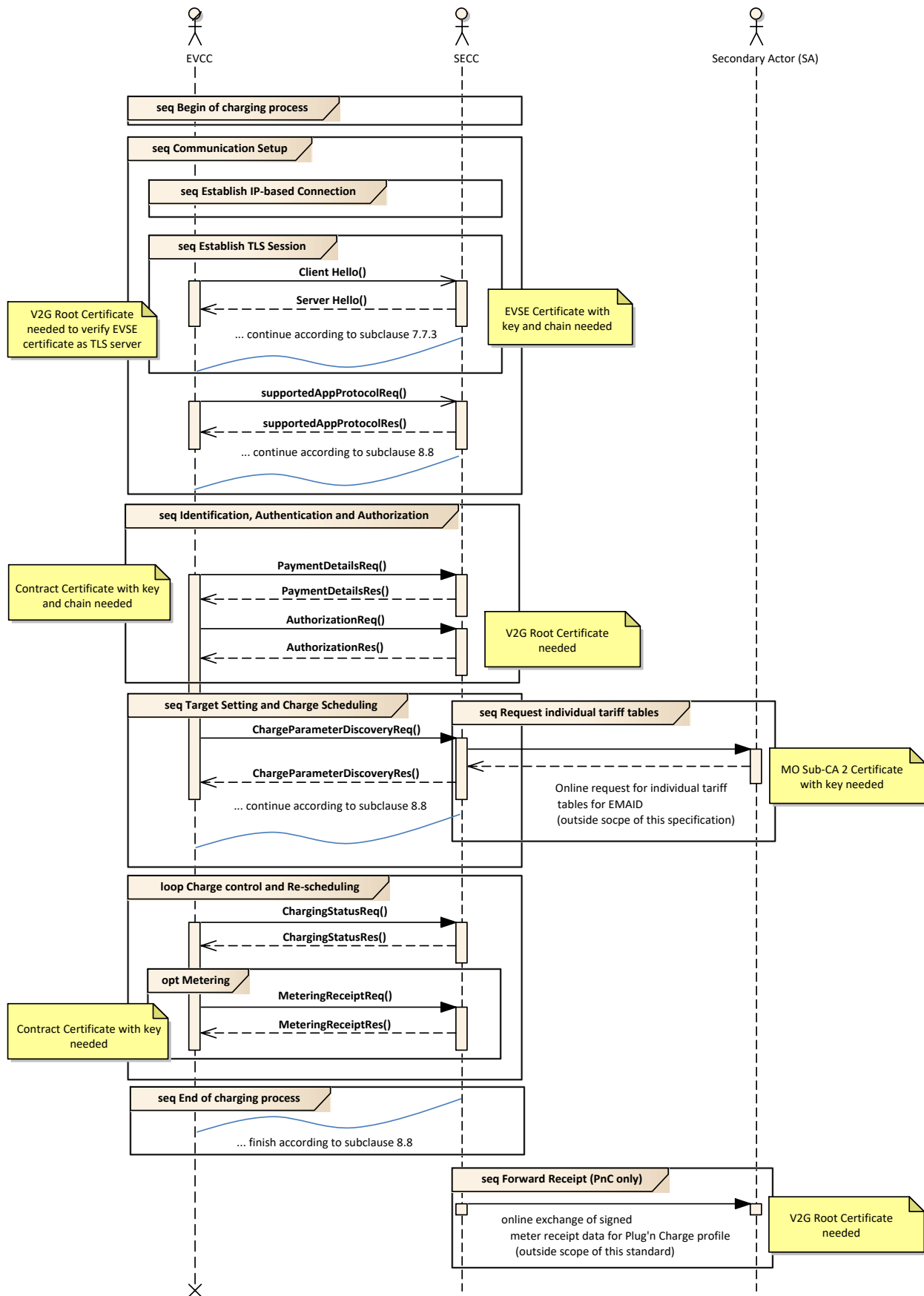


Figure 5 — Example for online communication

There are further use cases where security mechanism are needed on application layer. These are the initial enrolment 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 F.3. An overview on all needed certificates can be found in Annex B.

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 EVCC to authenticate SECC. There are contract certificates used at the application layer to authenticate against an SECC and/or secondary actor. 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.

[V2G2-004] Each V2G entity shall use X.509v3 certificates due to the need of extensions for storing EC-parameters. For details refer to IETF RFC 5280.

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, etc.)
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: Microsoft SGC (1.3.6.1.4.1.311.10.3.3) Netscape SGC (2.16.840.1.113730.4.1) SGC stands for Server Gated Crypto and indicates 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 response (exists only for SubCA certificates). 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.

[V2G2-005] Each V2G entity shall support hash-operation SHA-256 (signature process) according to NIST FIPS PUB 180-4 (use case element ID: F1 of ISO 15118-1).

[V2G2-006] For each V2G entity the signature operation shall be ECC-based using elliptic curves (secp256r1[SECG notation]) with signature algorithm ECDSA (use case element ID: F1 of ISO 15118-1).

[V2G2-1002] 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 as specified in detail in IETF RFC 4050 IETF RFC 4050:2005, section 3.3.

NOTE 3 The output of the ECDSA algorithm consists of a coordinate, which is a pair of integers, 'r' and 's'. As there is no length information for the encoded r- and s-value, the receiver will not be able to distinguish these values reliably, unless both values have the maximum length (256 bit).

[V2G2-007] The key length for ECC based asymmetric cryptography that is used by each V2G entity shall be 256 Bit.

[V2G2-885] All certificate validations shall be carried out in conformance with RFC 5280. The EVCC and the SECC may cache certificate validation results during one charging session.

- [V2G2-926]** The certificate extensions as determined in Annex B shall be supported. Deviations are specified where necessary.
- [V2G2-925]** 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.
- [V2G2-910]** The EVCC should implement a mechanism to check the validity periods of certificates and OCSP responses.
- [V2G2-886]** The EVCC may choose the accuracy of its time source at its own discretion, but it shall respect the chosen accuracy when using the time source. The accuracy should be at least one day.

This requirement theoretically even allows for precisions of, e.g. one year. It is up to the implementer to weigh the security consequences of such a decision.

If a TLS connection is built up successfully, the EVCC might use the time from a EVSETimeStamp field sent from the SECC through said connection for synchronization of its internal clock, however, it is up to the implementer to weigh the security consequences of such a decision.

- [V2G2-887]** 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

- [V2G2-008]** Each EVCC shall support at least one V2G root certificate.
- [V2G2-877]** 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 can exist, see V2G2-012.

Five V2G root certificates are strongly recommended. However, just one is mandatory. Having less than five or just one certificate brings a risk to the OEM. Having just one V2G root certificate allows the vehicle to charge just in that one region. If an OEM is afraid, that five V2G root certificate are not sufficient to cover the "usage radius" of its vehicles, OEM is free to provide more root certificate storage locations.

NOTE 2 It is assumed that the V2G root certificate applied on OSI layer 4 are also used on OSI layer 7. Additionally, it is assumed that in Europe will be a single root certificate authority like 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 five root certificates for five world-regions are sufficient. If one decides for more space for certificates this doesn't affect compatibility. For the SECC however it is mandatory to store more since there might be ten root certificates valid concurrently for each world-region.

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

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

- [V2G2-010]** The size of a certificate in DER encoded form shall be not bigger than 800 Bytes. For transmission, all certificates shall be DER encoded.
- [V2G2-011]** The validity period of any V2G root certificate shall be 40 years.
- [V2G2-012]** At any point in time there shall be a V2G root certificate available which is valid for each V2G root CA at least the next 35 years.

NOTE 4 For explanations of certificate validity, number of root certificates, certificate depth and size refer to F.1.

[V2G2-878] The maximum number of concurrently valid V2G root certificates for one root CA shall be never more than ten.

[V2G2-867] A V2G root shall not issue a leaf certificate.

NOTE 5 Leaf certificates can only be issued by a sub-CA.

[V2G2-869] 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.

[V2G2-911] 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 F.2 for a more detailed explanation.

[V2G2-882] Each EVCC shall be able to store at least one private operator root certificate which shall be replaceable by the vehicle owner.

[V2G2-927] The EVCC shall consider stored private operator root certificates as trust anchors for SECC certificate verification.

[V2G2-883] The validity times of SECC certificates having a trusted private operator root certificate as their trust anchor may be chosen by the certificate signer at his own discretion.

[V2G2-868] For a private environment, Sub-CAs and OCSP responses are not supported.

NOTE 6 That means, a private operator root certificate directly signs a leaf certificate.

7.3.4 Support and application of TLS

[V2G2-1028] The EVCC shall use TLS for identification mode PnC.

[V2G2-1029] The SECC shall use TLS for identification mode PnC.

Based on the transport layer setup of either TCP or TLS, the following restrictions apply:

[V2G2-632] If a V2G communication session without TLS is used, the SECC shall only provide the EIM identification mode and the message sets EIM charging AC or EIM charging DC by indicating "ExternalPayment" in the parameter PaymentOptionList of the ServiceDiscoveryRes message as defined in 8.4.3.3.3.

[V2G2-633] If a V2G communication session without TLS is used, the EVCC shall only accept the EIM identification mode with message sets EIM charging AC or EIM charging DC, no matter if the SECC offers also other identification modes.

[V2G2-634] If a V2G communication session without TLS is used, the SECC shall not provide the PnC message sets.

[V2G2-635] If a V2G communication session without TLS is used, the EVCC shall not apply the PnC message sets.

[V2G2-1031] If a V2G communication session without TLS is used, the SECC should not provide the message set VAS.

NOTE 1 Security measures for value added services enabled by the message set VAS (offered in ServiceDiscoveryRes) are not in scope of this document.

[V2G2-639] If TLS is not applied both sides shall ensure that an identification mode change from EIM to another identification mode and a message set change from EIM AC or EIM DC to another message set in the current charging session is not possible (avoiding security downgrade of the changed to session).

[V2G2-640] If TLS is applied both sides shall ensure that switching off TLS shall result in ending the charging session (avoiding security downgrade of the actual session).

The support, usage and restrictions regarding TLS are illustrated in Table 3 and Table 4.

Table 3 — TLS implementation/support for EIM identification modes

Allowed Message Sets ^a	Other environment (not trusted)		Trusted environment ^c	
	DC EIM	AC EIM	DC EIM	AC EIM
EVCC TLS support	optional	optional	optional	optional
SECC TLS support	mandatory	mandatory	optional	optional
TLS usage negotiation using SDP ^b	EV decides, EVSE shall accept EVs decision	EV decides, EVSE shall accept EVs decision	refer to Table 4	refer to Table 4
^a This refers to messages as defined in this document. In case of VAS, of course any other connections (which are not part of this document) are possible ^b Rejecting means to stop communication ^c See Clause 3 for a definition				

NOTE 2 Not supporting TLS in the SECC can lead in general to aborted charging sessions with particular EVs as it is in the responsibility of the EV to accept sessions without TLS.

NOTE 3 It is out of scope of this document to restrict the use of VAS in regards to TLS. The VAS application specification is responsible to specify whether TLS shall be used with that specific VAS or not.

Table 4 — SDP handshake with AC and DC EIM identification mode in trusted environment

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 establish 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 4 For the message set "EIM AC" and "EIM DC" it is in the responsibility of the EV to decide on not using TLS and accepting the risk of an unsecured connection.

NOTE 5 If TLS is applied, it is always used with unilateral (EVSE-side) authentication. If TLS is not used, there is no EVSE side authentication towards the EV as well as further protection of the communication channel on transport layer.

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 document does not imply any implementation. The figures in this subclause only show the basic sequencing for managing the protocol stack.

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

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

The following applies for the EVCC:

[V2G2-014] After a 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 7.6.3.2 and 7.6.3.3.

NOTE 1 Refer e.g. to ISO 15118-3 for the establishment of a data link layer connection.

[V2G2-016] The EVCC shall process the IP address assignment mechanism as defined in 7.6.3.2 and 7.6.3.3.

[V2G2-018] After a link-local IP address is assigned, the EVCC shall start the process for discovering the SECC address as defined in 7.10.1.

[V2G2-019] The EVCC shall start the SDP client according to 7.10.1.

[V2G2-645] 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.

[V2G2-021] If the EV decides to apply a secured connection, the EVCC shall establish the TLS connection to the SECC as described in 7.7.3 after the SECC IP address, port and available transport protocol and security options are discovered.

[V2G2-646] If the EV decides to apply an unsecured connection, the EVCC shall establish a TCP connection to the SECC as described in 7.7.1 after the SECC IP address, port and available transport protocol and security options are discovered.

[V2G2-022] Depending on [V2G2-021] and [V2G2-646], the EVCC shall attempt to establish a TLS or TCP connection according to 7.7.3.

[V2G2-1032] Once the TLS and/or TCP connection is established, the EVCC shall initiate the V2G communication session according to **[V2G2-1300]** in Clause 8.

[V2G2-1033] After having stopped the V2G communication session, the EVCC shall

- stop the TLS communication session by sending a "close_notify" alert and subsequently close the TCP connection by sending a FIN packet, or
- if no TLS is used: directly close the TCP connection by sending a FIN packet.

NOTE 2 In case of an error on the transport layer (TCP), an RST packet might be sent (refer to IETF RFC 793).

- [V2G2-1034]** If the EVCC sent the message SessionStopReq with parameter ChargingSession equal to "Terminate" it shall terminate the data link (D-LINK_TERMINATE.request()) within 5 s after having received the message SessionStopRes and after having closed the TLS and/or TCP connection. After that, the EVCC may continue with **[V2G2-721]** and try to establish a new V2G communication session.
- [V2G2-1035]** If the EVCC sent the message SessionStopReq with parameter ChargingSession equal to "Pause" it shall pause the Data-Link (D-LINK_PAUSE.request()) within 5 s after having received the message SessionStopRes and after having closed the TLS and/or TCP connection, and continue with **[V2G2-014]**. It shall then try to resume the paused V2G communication session.
- [V2G2-719]** Whenever the EVCC receives the indication for a missing Data-Link (D-LINK_READY.indication (DLINKSTATUS=No link), the EVCC shall continue with **[V2G2-014]**.
- [V2G2-1036]** If the EVCC identifies an error as specified in 8.7.3.2 and 8.8.4.2.1, it shall indicate a data link error (D-LINK_ERROR.request()) within 5 s and continue with **[V2G2-014]**. It shall then try to establish a new V2G communication session.

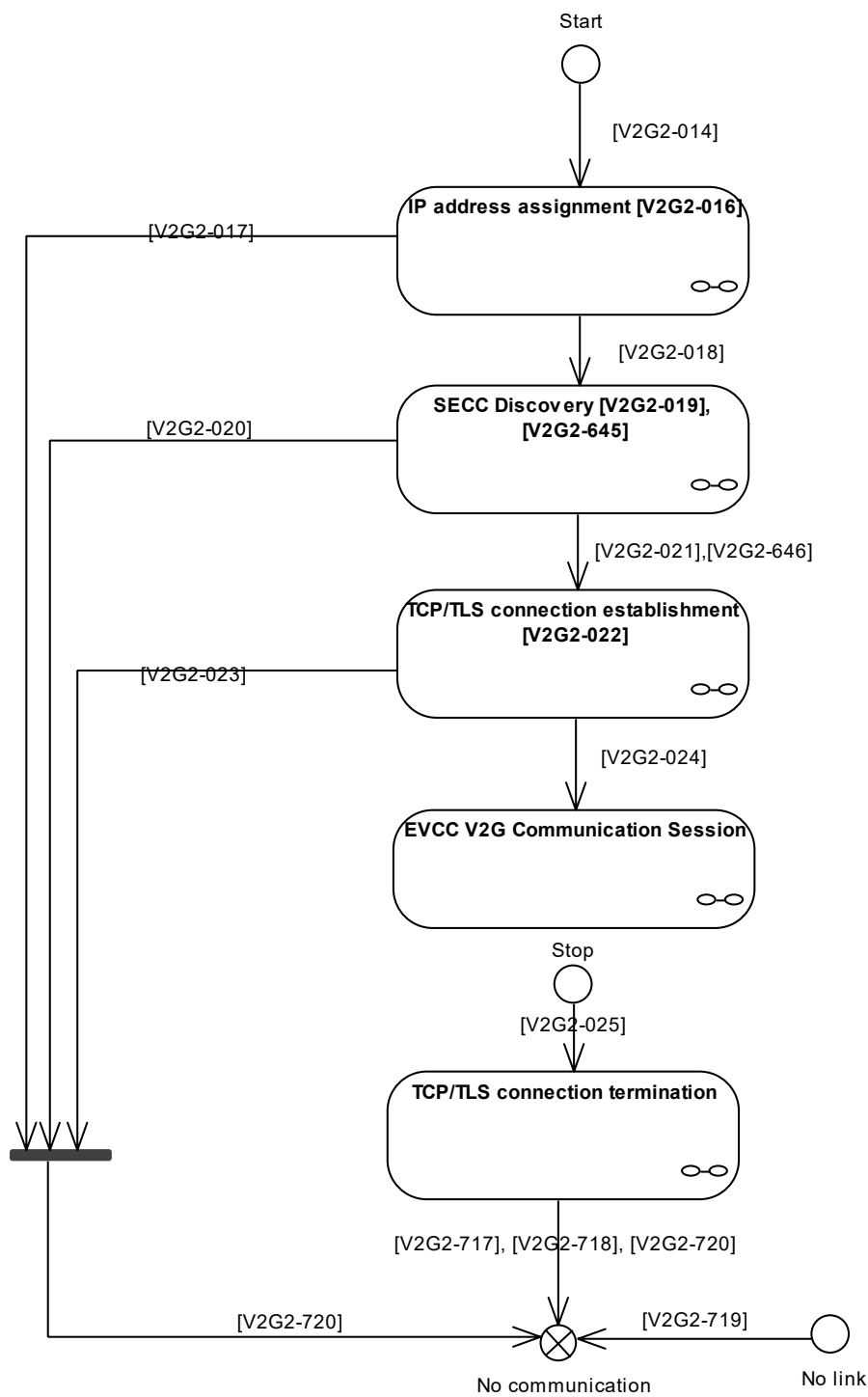


Figure 6 — Overview V2G communication states EVCC

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

The following applies for the SECC:

[V2G2-721] After a data link layer connection is established (D-LINK_READY.indication(DLINKSTATUS=Link established), the SECC shall initiate the IP address assignment mechanism as defined in 7.6.3.2 and 7.6.3.3.

NOTE 3 Refer e.g. to ISO 15118-3 for the establishment of a data link layer connection.

[V2G2-026] The SECC shall configure an IP address (static or dynamic) by any appropriate mechanism.

NOTE 4 To enable the integration of an SECC in different communication infrastructures, the definition of the address assignment for the SECC is not in scope of this document. This enables the operator to assign an appropriate mechanism. For example, the operator can choose any existing mechanism providing a valid IP address like, e.g. a static IP or the mechanism described in 7.6.3.2 and 7.6.3.3.

NOTE 5 The IP assignment mechanism for the SECC has no impact on compatibility and is not defined by this document.

[V2G2-027] After the IP address is assigned, the SECC shall start the SDP server as defined in 7.10.1.

NOTE 6 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.

[V2G2-030] 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 7.10.1.5.

[V2G2-031] The SECC shall wait until the TLS or TCP connection is established.

[V2G2-1037] Once the TLS or TCP connection is established, the SECC shall wait for the initialization of the V2G communication session according to [V2G2-1427].

[V2G2-722] If [V2G2-1037] applies the SECC may stop the SDP server after successful establishment of a TCP or TLS connection.

[V2G2-1038] After having stopped the V2G communication session with an error, the SECC shall

- stop the TLS communication session by sending a "close_notify" alert and subsequently close the TCP connection by sending a FIN packet, or
- if no TLS is used: directly close the TCP connection by sending a FIN packet.

NOTE 7 In case of an error on the transport layer (TCP), an RST packet might be sent.

[V2G2-1039] If the SECC received the message SessionStopReq with parameter ChargingSession equal to "Terminate" it shall terminate the data link (D-LINK_TERMINATE.request()) within 5 s after having sent the message SessionStopRes and after the TLS and/or TCP connection has been closed. After that, the SECC may continue with [V2G2-721] and try to establish a new V2G communication session.

[V2G2-1040] If the SECC received the message SessionStopReq with parameter ChargingSession equal to "Pause" it shall pause the Data-Link (D-LINK_PAUSE.request()) within 5 s after having sent the message SessionStopRes and after the TLS and/or TCP connection has been closed, and continue with [V2G2-721]. It shall then try to resume the paused V2G communication session.

[V2G2-726] Whenever the SECC receives the indication for a missing Data-Link (D-LINK_READY.indication (DLINKSTATUS=No link), the SECC shall continue with [V2G2-721].

[V2G2-1041] If the SECC identifies an error as specified in 8.7 and 8.8 it shall indicate a data link error (D-LINK_ERROR.request()) within 5 s and continue with [V2G2-721]. It shall then try to establish a new V2G communication session.

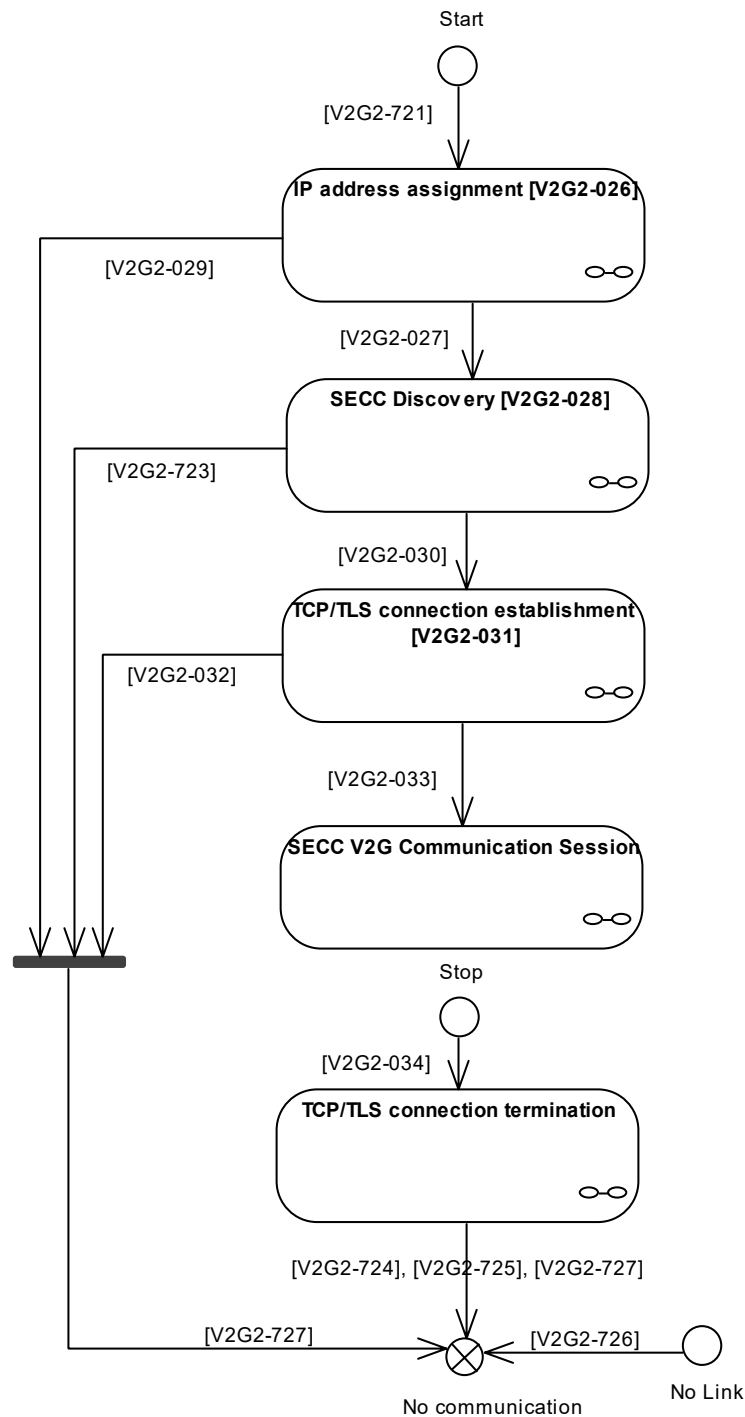


Figure 7 — Overview V2G communication session states SECC

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 defines additional details on data link layer to be covered.

[V2G2-035] If the EVCC communicates by PLC, the EVCC shall comply with ISO 15118-3.

[V2G2-036] If the SECC communicates by PLC, the SECC shall comply with ISO 15118-3.

7.6 Network layer

7.6.1 General

The protocol specified in this document 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

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

[V2G2-1030] While IETF RFC 2460 defines IPsec as mandatory, a V2G entity shall treat support of IPsec as optional.

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

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.

[V2G2-040] A V2G entity shall implement path MTU discovery according to IETF RFC 1630, Universal Resource Identifiers in WWW

IETF RFC 1981.

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

NOTE 1 A V2G entity complies with the specification in IETF RFC 5220, which extends IETF RFC 2460.

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

NOTE 2 The communication between EVCC and secondary actors is not in scope of this document but can use IP fragmentation.

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 using stateless auto address configuration (SLAAC), which is mandatory according to this document (refer to 7.6.3.2). DHCPv6 might be implemented as an optional IP configuration method.

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

[V2G2-044] If the infrastructure the EV is connected to (EVSE) chooses to implement a DHCPv6 server, it shall implement it according to IETF RFC 3315.

7.6.2.3 Neighbour discovery (ND)

The EVCC uses IPv6 stateless address auto configuration 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.

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

[V2G2-046] 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.).

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

[V2G2-049] 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	Neighbour solicitation	IETF RFC 4861
136	Neighbour advertisement	IETF RFC 4861
137	Redirect message	IETF RFC 4861
141	Inverse neighbour discovery solicitation message	IETF RFC 3122
142	Inverse neighbour 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 document:

- 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 can 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)

[V2G2-050] Each V2G entity shall support the configuration of a link-local IPv6 unicast address as specified in IETF RFC 4291.

[V2G2-051] 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.

[V2G2-052] The EVCC shall support auto configuration of IP6 addresses as described in IETF RFC 4862.

[V2G2-053] If the SECC provides the message sets “certificate installation”, “certificate update”, or “value added services” as defined in 8.6.2 it shall support IETF RFC 6106 for providing a DNS server address.

7.6.3.3 Address selection

[V2G2-054] 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. To exchange in a reliable way and in-order delivery of sender to receiver data. Additionally, TCP provides flow control and congestion control and furthermore provides various algorithms to handle congestion and influence flow control.

7.7.1.2 Applicable RFCs, limitations and protocol parameter settings

[V2G2-055] 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:

[V2G2-057] Each V2G entity should implement TCP congestion control according to IETF RFC 5681.

[V2G2-058] Each V2G entity should implement the NewReno modification to TCP's fast recovery algorithm according to IETF RFC 6582.

[V2G2-1042] Whenever a TCP retransmission timeout (RTO) is computed in a V2G entity, the RTO shall be lower than 200 ms.

[V2G2-1043] Whenever a TCP retransmission timeout (RTO) is computed in a V2G entity, the RTO should be in the range of 50 ms (lower bound) and 110 ms (upper bound).

[V2G2-060] To increase TCP's performance each V2G entity should implement TCP extensions for high performance according to IETF RFC 1323.

[V2G2-061] Each V2G entity should support TCP selective acknowledgment options according to IETF RFC 2018.

[V2G2-062] Each V2G entity should implement the user timeout option according to IETF RFC 5482.

[V2G2-063] The urgent pointer for TCP shall not be used by any V2G entity.

It is recommended to use the following checksum algorithm:

[V2G2-064] 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 15118-1:2019, Annex B for details on security use cases).

7.7.2.2 Applicable RFC, limitations and protocol parameter settings

[V2G2-065] 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

[V2G2-067] 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.

With unilateral authentication the EVCC authenticates the SECC according to [V2G2-067], 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 C1 and C2 in ISO 15118-1 (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 7.9.2.

7.7.3.3 Transport layer security usage

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

[V2G2-1019] Each EVCC may check the validity of the Sub-CA certificates (in the SECCs certificate chain) via an OSCP response according to IETF RFC 6960, when TLS is used. The OSCP requests should be transported as part of the TLS handshake using the extension defined in IETF RFC 6961.

NOTE 1 OSCP is not widely supported. The probability is high that an SECC will not support it. Requesting an OSCP response could prevent a successful TLS handshake and thus the start of a charging session.

NOTE 2 It is not intended that the EVCC requests an OSCP response for an SECC leaf certificate during TLS handshake.

NOTE 3 If the EV requests the OSCP response and the response is negative, [V2G2-875] still applies (EVCC will abort the TLS setup process).

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

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

NOTE 4 The pairing mode can be re-activated any time.

NOTE 5 The OEM is suggested to explain the usage and the threats of the pairing mode, e.g. in the user manual.

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

[V2G2-876] The validity period of an OSCP response for a Sub-CA 1 and Sub-CA 2 shall be no longer than 4 weeks.

NOTE 6 This is aligned to the validity period of an SECC leaf certificate.

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

NOTE 7 It is out of scope of this document how errors are handled. It is up to the OEM how these errors are handled.

[V2G2-651] 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.

[V2G2-871] 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 OSCP responses, for each certificate that the TLS server responds with, an OSCP response shall be sent to EVCC, as defined in IETF RFC 6961. The OSCP responder shall fill the field "certs" in the OSCP response (BasicOCSPResponse) structure according to IETF RFC 6960:2013, section 4.2.1. The SECC shall also send the certificate of the OSCP responder if it is not the corresponding Sub-CA itself.

NOTE 8 As defined in IETF RFC2560, an OSCP responder can either be the sub-CA itself, or it can 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.

[V2G2-923] If the SECC cannot provide a certificate with a chain up to one of the roots which the EVCC signalled 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).

[V2G2-924] 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.

[V2G2-872] 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 9 This supports the “pairing mode”

[V2G2-873] 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.

[V2G2-874] 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 fulfils 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.

[V2G2-875] 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.

NOTE 10 After that, the SECC will proceed according to [V2G2-1152] and [V2G2-1153].

[V2G2-810] The SECC shall support maximum fragment length negotiation according to IETF RFC 6066.

[V2G2-811] The SECC shall be able to support, but not be limited to a maximum fragment length of 2^9 Bytes according to IETF RFC 6066.

7.7.3.4 Transport layer security credentials and cipher suites

For transport layer security, EVCC authenticates SECC using SECC certificate. This is being achieved by SECC having a private key corresponding to SECC certificate, and EVCC having V2G root certificate and verifying the certificate chain from the V2G root certificate to the SECC certificate. The validity check of Sub-CA certificate in the certificate chain is performed via the OCSP response received during TLS-handshake (for details refer to IETF RFC 6066). Mechanisms to revoke SECC certificates are not required but instead, it is required to be short term certificates.

As SECC is not aware of which V2G root certificate EVCC has, among 10 currently valid V2G root certificates for one region, thus 50 currently valid V2G root certificates worldwide. Therefore, it is necessary for EVCC to provide a list of V2G root certificates that EVCC possess through TLS handshake. SECC provides a certificate chain of its own SECC certificate whose root certificate is possessed by EVCC, together with OCSP response for the Sub-CA certificate in the chain. It is strongly recommended that the OCSP response is refreshed at least every week.

The communicated message between EVCC and SECC is encrypted using a symmetric key (one-way “key agreement”) negotiated during the TLS key negotiation phase. Therefore, the message will not be eavesdropped and both EVCC and SECC can be certain that the opponent is indeed identical throughout the session. (There can be no session hijacking.)

[V2G2-071] Each V2G entity shall provide the credentials and security information stated in Table 6, if TLS is used.

Table 6 — TLS authentication

TLS Authentication	Requirements to EVCC	Requirements to SECC
Unilateral (server side)	Availability of root certificates to check the authenticity of the SECC certificate Functional support for OCSP request/response processing to check the validation state of the SECC certificate during TLS handshake	SECC certificate and corresponding private key OCSP response to provide information about the validation state of own SECC certificate The SECC shall cache and store internally OCSP responses for its own chain of sub-cs certificates regularly (at least once per week).

[V2G2-602] The SECC shall support all cipher suites defined in Table 7, if TLS is used.

[V2G2-1044] The EVCC shall offer only TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 in ClientHello.

[V2G2-1045] Additional cipher suites may be supported by any V2G entity, as long as they are stronger than the ones mentioned in Table 7.

NOTE The OEM can decide which cipher suite the EVCC supports, based on the offer as described in Table 7. One is sufficient allowing for compact implementations. For interoperability, of course, the SECC supports all cipher suites as listed in Table 7.

Table 7 — Supported cipher suites

Cipher suite	RFC
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	IETF RFC 5289
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	IETF RFC 5289

7.8 V2G transfer protocol

7.8.1 General

The V2G transfer protocol (V2GTP) is a compact communication protocol to transfer V2G messages between two V2GTP entities. It mainly consists of a header and payload definition that allows to separate and process V2G messages efficiently. V2GTP is the document transfer protocol between the EVCC and SECC but may also be used for communication with other V2G Entities that support the V2GTP protocol.

7.8.2 Supported ports

V2GTP is based on TLS+TCP. TLS+TCP uses a pair of IP addresses (source address and destination address) and a pair of port numbers (source port and destination port) to establish and identify a connection for bidirectional exchange of byte streams. The connection is established from the source address and source port to the destination address and destination port. The ports listed in Table 8 are used by V2GTP entities.

Table 8 — Supported TCP ports for V2GTP

Name	Protocol	Port number	Description
V2G_SRC_TCP_DATA	TCP(unicast)	Port number in the range of dynamic ports (49152-65535) as defined in IETF RFC 6335.	V2GTP source port at a primary actor (e.g. EVCC) that implements the V2GTP protocol.
V2G_DST_TCP_DATA	TCP (unicast)	Port number at V2GTP entity providing a V2GTP destination port number in the range of dynamic ports (49152-65535) as defined in IETF RFC 6335. For a SECC it will be dynamically assigned by the SDP mechanism (7.10.1)	V2GTP destination port at a primary actor (e.g. SECC)

For V2GTP entities implementing the V2GTP the following general requirements apply:

[V2G2-073] A V2GTP entity providing a destination port shall support at least one connection on the local port V2G_DST_TCP_DATA as defined in Table 8.

[V2G2-074] A V2GTP entity providing a destination port may support multiple simultaneous connections on the local port V2G_DST_TCP_DATA as defined by Table 8.

[V2G2-075] A V2GTP entity using a source port shall support at least one connection on the local port V2G_SRC_TCP_DATA as defined in Table 8.

[V2G2-076] A V2GTP entity using a source port may support multiple connections on the local port V2G_SRC_TCP_DATA as defined in Table 8.

Especially, for an EVCC and an SECC the following applies:

[V2G2-077] The EVCC shall use a source port V2G_SRC_TCP_DATA as defined in Table 8.

[V2G2-078] The SECC shall provide a destination port V2G_DST_TCP_DATA as defined in Table 8.

[V2G2-079] The EVCC shall support at least one connection for a V2G communication session on port V2G_SRC_TCP_DATA.

[V2G2-080] The SECC shall support at least one connection for a V2G communication session on port V2G_DST_TCP_DATA.

[V2G2-081] The EVCC shall use the port V2G_DST_TCP_DATA returned in the last SECC Discovery response message (refer to sub-clause 7.10.1.5) for connecting the SECC

7.8.3 Protocol data unit

7.8.3.1 Structure

The V2GTP PDU consists of a header and a body section as shown in Figure 8.

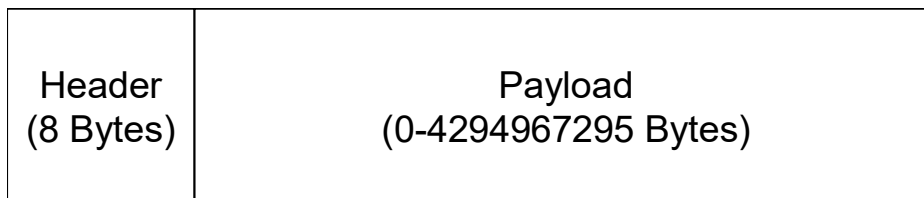


Figure 8 — V2GTP Message structure

The payload contains the application data (e.g. a V2G message). The header separates the payloads (i.e. individual V2GTP messages) within a byte stream and gives information for the payload processing.

The V2GTP message header structure is shown in Figure 9 and described in Table 9. The supported payload types are described in

Table 10.

Byte No.	1	2	3	4	5	6	7	8
Header Field	Protocol Version	Inverse Protocol Version	Payload Type		Payload Length			

Figure 9 — V2GTP Message header structure

[V2G2-082] A V2GTP entity shall use the header structure as shown in Figure 9.

[V2G2-083] A V2GTP entity shall send the 8 bytes of the V2GTP header in the order as shown in Figure 9.

[V2G2-084] A byte with a lower number shall be sent before a byte with a higher number. The header starts with byte 1 and ends with byte 8.

[V2G2-085] A V2GTP entity shall send the fields “payload type” and “payload length” in big endian format: The most significant byte is sent first, the least significant byte is sent last.

Table 9 — Generic V2GTP header structure

Header field	Header field description	Header field values
Protocol Version	Identifies the protocol version of V2GTP messages.	0x01: V2GTP version 1 0x00, 0x02-0xFF: reserved by document
Inverse Protocol Version	Contains the bit-wise inverse value of the protocol version which is used in conjunction with the V2GTP protocol version as a protocol verification pattern to ensure that a correctly formatted V2GTP message is received. Equals the <Protocol_Version> XOR 0xFF	0xFE: V2GTP Version 1
Payload Type (GH_PT)	Contains information about how to decode the payload following the V2GTP header.	Refer to Table 10 for a complete list of payload type values.
Payload Length (GH_PL)	Contains the length of the V2GTP message payload in bytes (i.e. excluding the generic V2GTP header bytes).	0...4294967295 (= <d>)

Table 10 — Overview on V2GTP payload types

Payload type value	Payload type name	Specified in subclause
0x0000 - 0x8000	Reserved	not applicable
0x8001	EXI encoded V2G message	7.9.1.2
0x8002 - 0x8FFF	Reserved	not applicable
0x9000	SDP request message	7.10.1.4
0x9001	SDP response message	7.10.1.5
0x9002 - 0x9FFF	Reserved	not applicable
0xA000 - 0xFFFF	Manufacturer specific use	not applicable

[V2G2-086] A V2GTP entity shall use the V2GTP message structure as shown in Figure 8 to send V2G messages as defined in Clause 8.

[V2G2-087] A V2GTP entity shall use the definitions as defined in Table 9 and Table 10.

[V2G2-088] For EXI encoded V2G messages (payload 0x8001) a V2GTP entity shall use a separate V2GTP message for each V2G message.

NOTE Requirement [V2G2-088] implies that the payload field can include neither a part of a message nor multiple messages.

7.8.3.2 Header processing

For the processing of the payload the V2GTP entity processes the header first. For this, a V2GTP entity that receives a V2GTP message checks the header field step by step. The header processing as defined below is illustrated in Figure 10.

[V2G2-089] A V2GTP entity shall process the V2GTP header as defined in Table 9 before processing the payload as defined in Table 10.

[V2G2-090] A V2GTP entity shall check the protocol version and inverse protocol version fields (synchronization pattern) before any other header fields.

[V2G2-092] A V2GTP entity shall check the payload type after the successful check of the version and inverse version field.

[V2G2-094] A V2GTP entity shall check the payload length after the successful check of the payload type.

[V2G2-096] If the header processing was successful the V2GTP entity shall process the payload.

[V2G2-800] If the V2GTP header contains wrong data (e.g., not supported payload type, wrong payload length, or not supported V2GTP version) the V2GTP entity shall ignore this message.

NOTE This approach increases robustness of the V2G charging session. If the proper message with correct data in the header is received before the respective timeout, the session can be continued. If not, the session will be stopped due to a timeout.

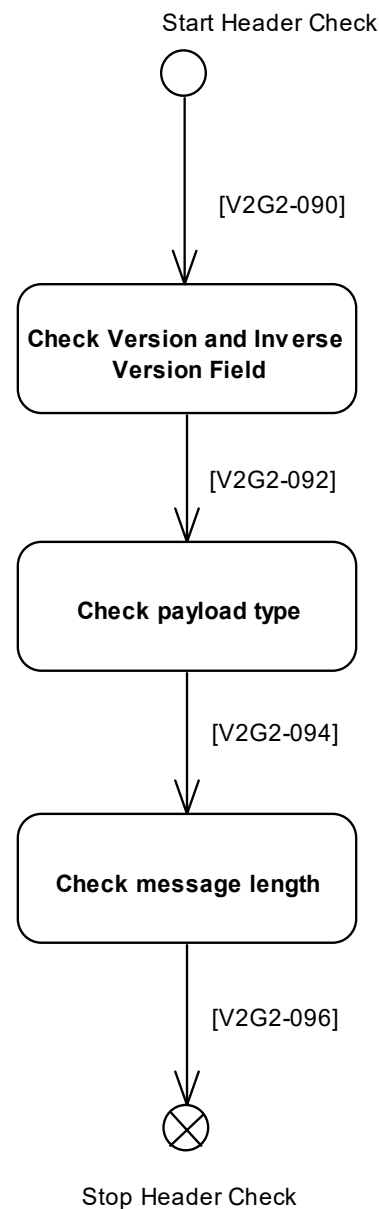


Figure 10 — V2GTP generic header handler

7.9 Presentation layer

7.9.1 XML and efficient XML interchange (EXI)

7.9.1.1 Overview

For the purpose of describing the V2G message set the presentation layer uses the widely adopted XML data representation accordingly the document defines messages (i.e. data structures and data types) based on XML schema which allows the type aware use of XML and enables simplified validity evaluation of exchanged messages.

[V2G2-097] When transmitting V2G messages defined in this document by using XML all V2G entities shall use encoding format according to definitions in W3C EXI 1.0.

7.9.1.2 Efficient XML interchange

The efficient XML interchange (EXI) format allows to use and process XML-based messages on a binary level. Thus, the EXI format increases the processing speed of XML-based data as well as reduces the memory usage. Basically, EXI is a W3C recommendation. The EXI format uses a relatively simple grammar driven approach that achieves very efficient encodings for a broad range of use cases. It is not uncommon for EXI messages to be up to 100 times smaller than equivalent XML documents. The EXI specification describes in a predefined process how schema information should be transformed into EXI grammar. The reason for doing so is that EXI grammar is much simpler to process, compared to XML Schema information. Nevertheless, the parsing can be performed in the same accurate way as it is possible in XML.

There are different kinds of coding mechanism with EXI. To meet the demands in ISO 15118 in terms of efficient processing, less resources usage, message size, and message extendibility schema-aware settings should be selected (see 7.9.1.3 for the requirement EXI settings for ISO 15118).

In general, EXI streams can be created in a very efficient way if all encoded information (elements/attributes) are defined by an underlying XML Schema (*Schema-informed Grammars*). Deviant information based on XML Schema knowledge is encoded in a more generic way. The EXI coder encodes the qualified names (namespace and element/attribute name) of such unknown information in a string-based manner. However, simple types of the schema deviations may be still encoded type-aware.

EXI decoders can decode the efficient EXI streams by using the same underlying XML Schema which was used for the encoding process. Schema deviations are recognized in the EXI stream. These deviations (unknown elements or attributes) can be either processed or skipped.

Figure 11 summarizes the Efficient XML Interchange concept for the ISO 15118 domain. Due to the high limited resource restriction the EVCC may only be able to handle the XML-based data using a corresponding data structure representation. Such data structures can be used to serialize or deserialize ISO 15118 application messages. Meanwhile, the SECC may be able to handle the data as data structure and/or the more resource intensive Document Object Model (DOM) or in a traditional plain-text XML variant.