
**Road vehicles — Vehicle to grid
communication interface —**

**Part 20:
2nd generation network layer and
application layer requirements**

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

*Partie 20: Exigences des couches réseau et application de 2ème
génération*



Reference number
ISO 15118-20:2022(E)

Documents
Document Sharing Hub
© ISO 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO 2022

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

Page

Foreword.....	v
Introduction.....	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions.....	4
4 Abbreviated terms	12
5 Conventions	15
5.1 Definition of OSI based services	15
5.2 Requirement structure.....	15
5.3 Usage of references.....	16
5.4 Notation used for XML schema diagrams.....	16
6 Document overview	16
7 Basic requirements for V2G communication.....	17
7.1 General information	17
7.2 Service primitive concept of OSI layered architecture	18
7.2.1 Overview	18
7.2.2 Syntax of service primitives.....	18
7.3 Security concept.....	19
7.3.1 General	19
7.3.2 Certificate and key management	21
7.3.3 Number of root certificates and root validity.....	35
7.3.4 Support and application of TLS	37
7.3.5 Firewall	38
7.3.6 Protection of the cryptographic keys	38
7.3.7 Random number generation	40
7.4 V2G communication states and data link handling.....	42
7.5 Data link layer.....	46
7.5.1 Data link layer security for WLAN	46
7.6 Network link layer	51
7.6.1 General	51
7.6.2 Applicable RFCs, limitations and protocol parameter settings	51
7.6.3 IP addressing.....	53
7.7 Transport layer	54
7.7.1 Transmission control protocol (TCP)	54
7.7.2 User datagram protocol (UDP)	55
7.7.3 Transport layer security (TLS)	56
7.8 V2G transfer protocol.....	82
7.8.1 General information	82
7.8.2 Supported ports	83
7.8.3 Protocol data unit.....	84
7.9 Presentation layer.....	87
7.9.1 XML and efficient XML interchange (EXI)	87
7.9.2 Message security.....	90
7.10 Application layer.....	115
7.10.1 SECC discovery protocol.....	115
8 Application layer messages	128
8.1 General information and definitions.....	128
8.2 Protocol handshake definition	129

8.2.1	Handshake sequence	129
8.2.2	Message definition supportedAppProtocolReq and supportedAppProtocolRes	131
8.2.3	Semantics description supportedAppProtocol messages	132
8.2.4	Message examples	133
8.3	V2G message definition	134
8.3.1	Overview	134
8.3.2	General	135
8.3.3	Header definition	135
8.3.4	Request and response definitions	138
8.3.5	Complex data types	240
8.4	Service selection	361
8.4.1	General	361
8.4.2	General description of configuration parameters	362
8.4.3	Selection of service and service parameters	363
8.5	V2G communication timing	373
8.5.1	Overview	373
8.5.2	Common	373
8.5.3	DC service	374
8.5.4	Message sequence and communication session	374
8.5.5	Session setup and ready to charge	381
8.5.6	V2G message synchronization for AC and DC with IEC 61851-1 signalling	387
8.5.7	V2G message synchronization with IEC 61980-2 signalling for WPT	394
8.6	Message sequencing and error handling	394
8.6.1	Overview	394
8.6.2	Basic definitions for error handling	395
8.6.3	ResponseCode handling	395
8.6.4	Request-response message sequence requirements	406
8.6.5	Multiplexed communication	434
8.6.6	Message sequence diagrams	437
	Annex A (normative) Schema definition	442
	Annex B (normative) Certificate profiles	444
	Annex C (normative) Specification of identifiers	498
	Annex D (informative) ACDP	504
	Annex E (informative) Basic PPD for interoperability	506
	Annex F (informative) Message sequencing for renegotiation	509
	Annex G (informative) Association of VAS client to V2G session	511
	Annex H (informative) Application of certificates	512
	Annex I (informative) Precision of measurements and tolerances	547
	Annex J (informative) Absolute pricing examples	549

Foreword

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

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

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

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

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

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

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

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

Introduction

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

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

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

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

It includes:

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

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

Road vehicles — Vehicle to grid communication interface —

Part 20: Network and application protocol requirements

1 Scope

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

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

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

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

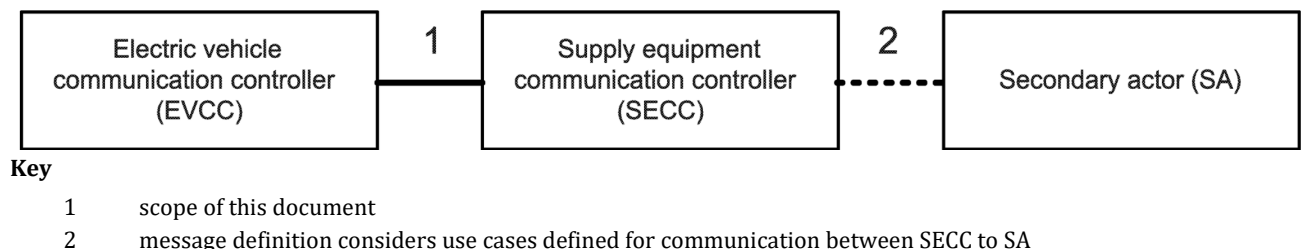


Figure 1 — Communication relationship among the EVCC, SECC and SA

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

2 Normative references

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

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

ISO 4217, *Codes for the representation of currencies*

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

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

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

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

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

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

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

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

IEC 63119-2¹, *Information exchange for Electric Vehicle charging roaming service — Part 2: Use cases*

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

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

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

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

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

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

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

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

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

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

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

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

¹ Under preparation. Stage at the time of publication: IEC/CCDV 63119-2:2022.

- IETF RFC 4514, *Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names* (June 2006)
- IETF RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)* (September 2007)
- IETF RFC 4862, *IPv6 Stateless Address Autoconfiguration* (September 2007)
- IETF RFC 5116, *An Interface and Algorithms for Authenticated Encryption* (January 2008)
- IETF RFC 5216, *The EAP-TLS Authentication Protocol* (March 2008)
- IETF RFC 5234, *Augmented BNF for Syntax Specifications: ABNF* (January 2008)
- IETF RFC 5480, *Elliptic Curve Cryptography Subject Public Key Information* (March 2009)
- IETF RFC 5722, *Handling of Overlapping IPv6 Fragments* (December 2009)
- IETF RFC 6066, *Transport Layer Security (TLS) Extensions: Extension Definitions* (January 2011)
- IETF RFC 6724, *Default Address Selection for Internet Protocol version 6 (IPv6)* (September 2012)
- IETF RFC 6818, *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* (January 2013)
- IETF RFC 6874, *Representing IPv6 Zone Identifiers in Address Literals and Uniform Resource Identifiers* (February 2013)
- IETF RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP* (June 2013)
- IETF RFC 7405, *Case-Sensitive String Support in ABNF* (December 2014)
- IETF RFC 7748, *Elliptic Curves for Security* (January 2016)
- IETF RFC 8032, *Edwards-Curve Digital Signature Algorithm (EdDSA)* (January 2017)
- IETF RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification* (July 2017)
- IETF RFC 8201, *Path MTU Discovery for IP version 6* (July 2017)
- IETF RFC 8398, *Internationalized Email Addresses in X.509 Certificates* (May 2018)
- IETF RFC 8399, *Internationalization Updates to RFC 5280* (May 2018)
- IETF RFC 8415, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)* (November 2018)
- IETF RFC 8439, *ChaCha20 and Poly1305 for IETF Protocols* (June 2018)
- IETF RFC 8446, *The Transport Layer Security (TLS) Protocol Version 1.3* (August 2018)
- IETF RFC 8504, *IPv6 Node Requirements* (January 2019)
- IETF RFC 8335, *PROBE: A Utility for Probing Interfaces* (February 2018)
- ANSI X9.62, *Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)* (2005)

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

IANA Service & Port Registry, *Service Name and Transport Protocol Port Number Registry* [viewed 2011-01-16], Available from: <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml>

NIST FIPS PUB 180-4, *Secure Hash Standard (SHS)* (March 2012)

NIST FIPS PUB 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions* (August 2015)

ITU-T X.509, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks* (October 2019)

IEEE 802.1X-2020, *IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control* (January, 2020)

WPA3, *WPA3 Specification Version 3.0* (December 2020)

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

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

3 Terms and definitions

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

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

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

3.1 access point

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

3.2 authorization mode

authenticate and authorize the user account

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

3.3 automatic connection device pantograph

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

3.4 basic charging

BC

charging based on PWM

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

3.5**certificate**

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

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

3.6**charging limit**

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

EXAMPLE Voltage, current, energy, power, etc.

3.7**charging session**

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

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

3.8**charging station operator****CSO**

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

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

3.9**communication session**

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

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

3.10**communication setup timer**

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

3.11**contract certificate**

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

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

3.12

CP state

control pilot state

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

3.13

credential

piece of information attesting an entity's identity

3.14

cross certificate

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

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

3.15

distinguished encoding rules

DER

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

3.16

dynamic control mode

control mode for the communication

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

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

3.17

external identification means

EIM

authorization means that are handled outside of this document

3.18

elliptic curve cryptography

ECC

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

3.19

eMobility account identifier

EMAID

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

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

3.20

eMobility service provider

eMSP

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

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

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

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

3.21

electric vehicle communication controller

EVCC

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

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

3.22

EVPowerProfile

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

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

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

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

3.23

electric vehicle supply equipment ID

EVSEID

unique identification of the EVSE

3.24

electric vehicle supply equipment

EVSE

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

3.25

electric vehicle supply equipment

EVSE

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

3.26

global address

IP address (3.28) with unlimited scope

3.27

high level communication charging

HLC-C

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

3.28

IP address

address

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

3.29

link-local address

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

3.30

maximum transfer unit

MTU

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

3.31

message set

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

3.32

message timer

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

3.33

meter

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

3.34

multiplexed communication

MC

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

3.35

node

device that implements IPv6

3.36

original equipment manufacturer

OEM

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

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

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

3.37

OEM provisioning certificate

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

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

3.38**PE certificate**

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

3.39**PE EVSE**

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

3.40**performance time**

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

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

3.41**park and charge****PnC**

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

3.42**private environment****PE**

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

3.43**private SECC**

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

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

3.44**public SECC**

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

3.45**request-response message pair**

request message and the corresponding response message

3.46**request-response message sequence**

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

3.47

supply equipment communication controller

SECC

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

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

3.48

SECC certificate

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

3.49

sequence timer

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

3.50

service session

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

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

3.51

scheduled control mode

control mode for the communication

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

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

3.52

schedule renegotiation

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

3.53

station

STA

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

3.54

SDP client

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

3.55

SDP server

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

3.56

smart meter

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

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

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

3.57

sub-CA

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

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

3.58

sub-CA certificate

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

3.59

TCP_DATA

socket interface for data transfer based on TCP connection

3.60

timeout

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

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

3.61

timer

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

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

3.62

vehicle certificate

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

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

3.63

vehicle to grid

V2G

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

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

3.64

V2G communication session

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

3.65

V2G entity

primary actor participating in the V2G communication

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

3.66

V2G message

message exchanged on application layer

Note 1 to entry: Refer to Clause 8.

3.67

V2G setup

setup phase for V2G messaging

3.68

V2G transfer protocol

V2GTP

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

3.69

V2GTP entity

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

3.70

V2G root CA

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

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

3.71

V2G root CA certificate

certificate issued to *V2G root CA* (3.70)

4 Abbreviated terms

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

AC	alternating current
ACDP	automatic connection device pantograph
CPDA	DC_ChargeParameterDiscovery
AKI	authority key identifier
AP	access point
APOS	ACDP_VehiclePositioning
ASUP	AuthorizationSetup

AUTH	authorization
BEV	battery electric vehicle
BPT	bidirectional power transfer
CA	certificate authority
CC	CableCheck
CINS	CertificateInstallation
CONA	ACDP_Connect
CPM4PE	certificate provisioning mode for private environment
CPS	certificate provisioning service
CRL	certificate revocation list
CSO	charging station operator
DC	direct current
DCCL	DC_ChargeLoop
DH	Diffie Hellman
DER	distinguished encoding rules
DISA	DisconnetACDP
EAP	extensible authentication protocol
ECDSA	elliptic curve digital signature algorithm
EdDSA	Edwards-curve digital signature algorithm
EMA	e-mobility account
EMAID	e-mobility account identifier
EMOCH	e-mobility operator clearing house
eMSP	eMobility service provider
ESDW	emergency shut down
EV	electric vehicle
EVCC	electric vehicle communication controller
EVRESS	electric vehicle rechargeable energy storage system
EVSE	electric vehicle supply equipment

EVSEID	electric vehicle supply equipment identification
EXI	efficient XML interchange
HLC-C	high level communication charging
IV	initialization vector
MCON	MeteringConfirmation
NACK	negative acknowledgement
OCSP	online certificate status protocol
OEM	original equipment manufacturer
OID	object identifier
PC	PreCharge
PD(Start)	PowerDelivery(Start)
PD(Stop)	PowerDelivery(Stop)
PDU	protocol data unit
PE	private environment
PHEV	plug-in hybrid electric vehicle
PKI	public key infrastructure
PLC	power line communication
PMF	protected management frames
PnC	park and charge
PPD	pairing and positioning device
RFC	request for comments(IETF)
SA	secondary actor
SAID	secondary actor ID
SAP	SupportedAppProtocol
SDE	ServiceDetails
SDI	ServiceDiscovery
SDP	SECC discovery protocol
SDU	service data unit

SE	ScheduleExchange
SECC	supply equipment communication controller
SKI	subject key identifier
SOC	state of charge
SSEL	ServiceSelection
SSU	SessionSetup
SSP	SessionStop
SYSS	ACDP_SystemStatus
TCP	transmission control protocol
UDP	user datagram protocol
VAS	value added service
V2G	vehicle to grid

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

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

5 Conventions

5.1 Definition of OSI based services

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

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

5.2 Requirement structure

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

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

[V2G20-xxxx] requirement text, where:

- "V2G20" represents this document;

- "xxxx" represents the unique requirement number consisting of four digits starting from 1 000;
- "requirement text" defines the actual text of the requirement.

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

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

[V2G20-yyy] requirement text, where:

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

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

5.3 Usage of references

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

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

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

5.4 Notation used for XML schema diagrams

This document makes use of XML as a description format for V2G messages. For details with regards to the XML schema diagram notation used in this document refer to Reference [96].

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

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

6 Document overview

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

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

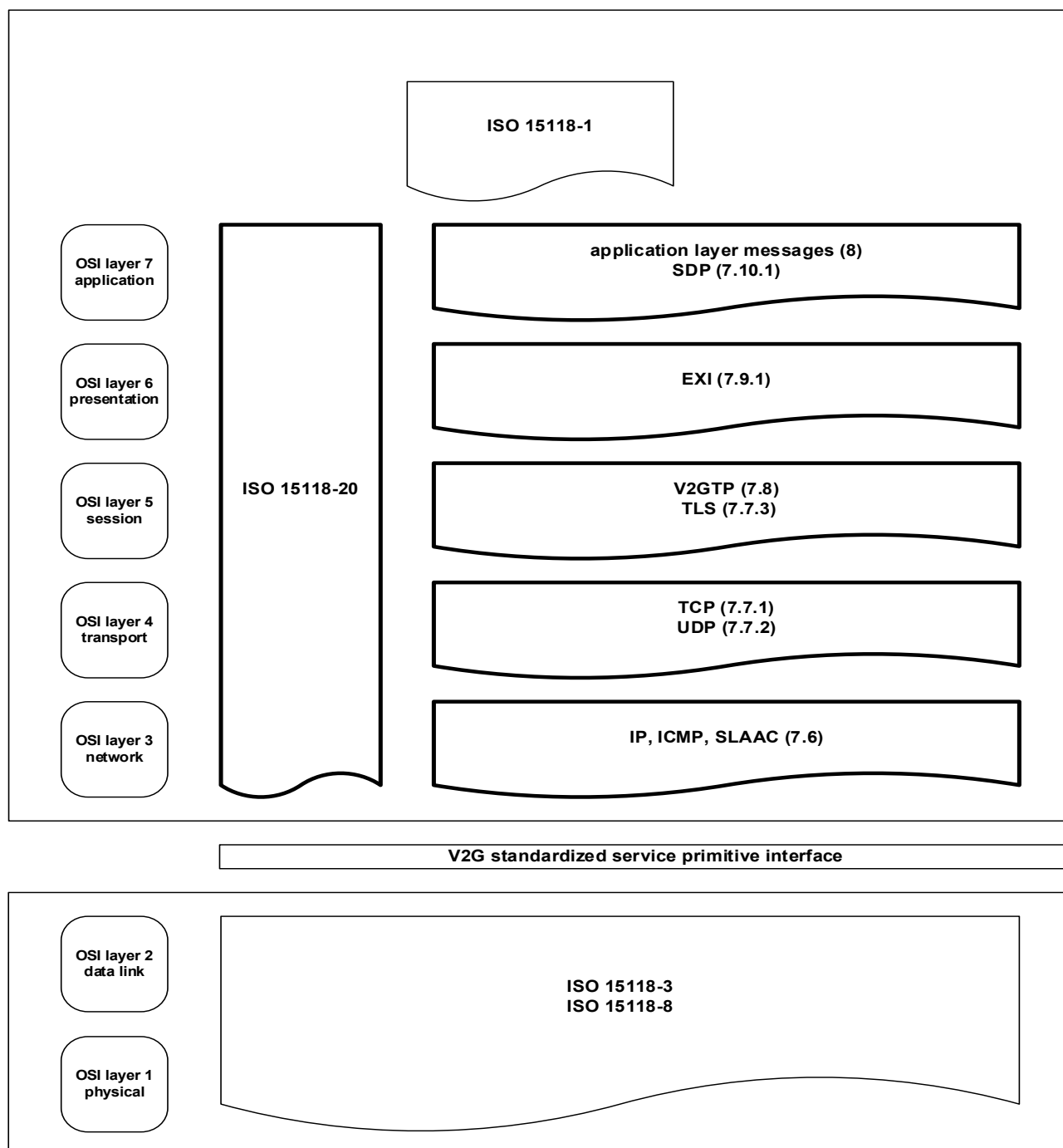


Figure 2 — Vehicle to grid communication document overview

7 Basic requirements for V2G communication

7.1 General information

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

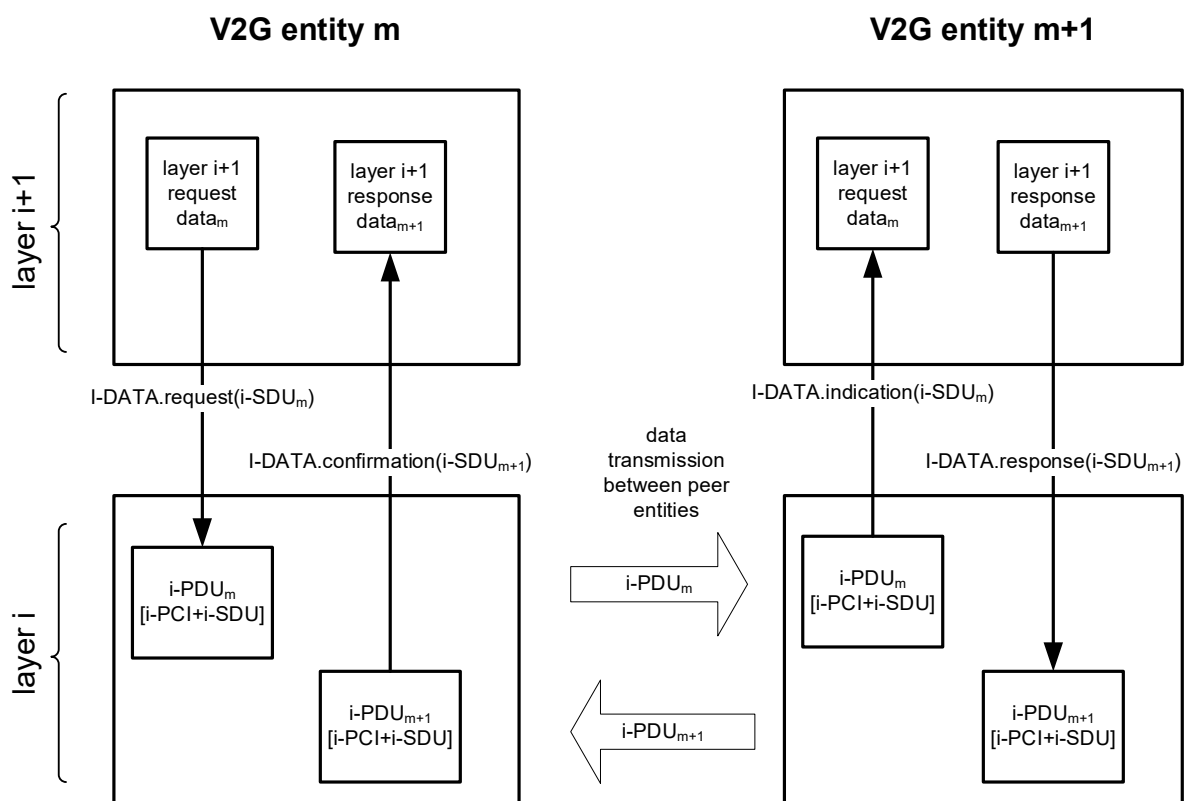
7.2 Service primitive concept of OSI layered architecture

7.2.1 Overview

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

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

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



Key

PDU_x: protocol data unit of network entity x
 PCI: protocol control information
 SDU_x: service data unit of network entity x

Figure 3 — OSI layered architecture principles

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

7.2.2 Syntax of service primitives

Service primitives are described with the following syntax:

- [Initial of layer]-[NAME].[primitive type](parameter list);

- a) whereas [initial of layer] is one out of the following seven:
 - physical, data link, network, transport, session, presentation, application;
- b) whereas [NAME] is the name of the primitive;

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

- c) whereas [primitive type] is one out of the following four:
 - request, indication, response, confirmation;
- d) whereas (parameter list) includes a list of parameters separated by comma the user of the service is supposed to provide when using the respective service primitive; optional parameters are marked with brackets "[..]".

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

7.3 Security concept

7.3.1 General

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

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

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

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

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

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

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

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

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

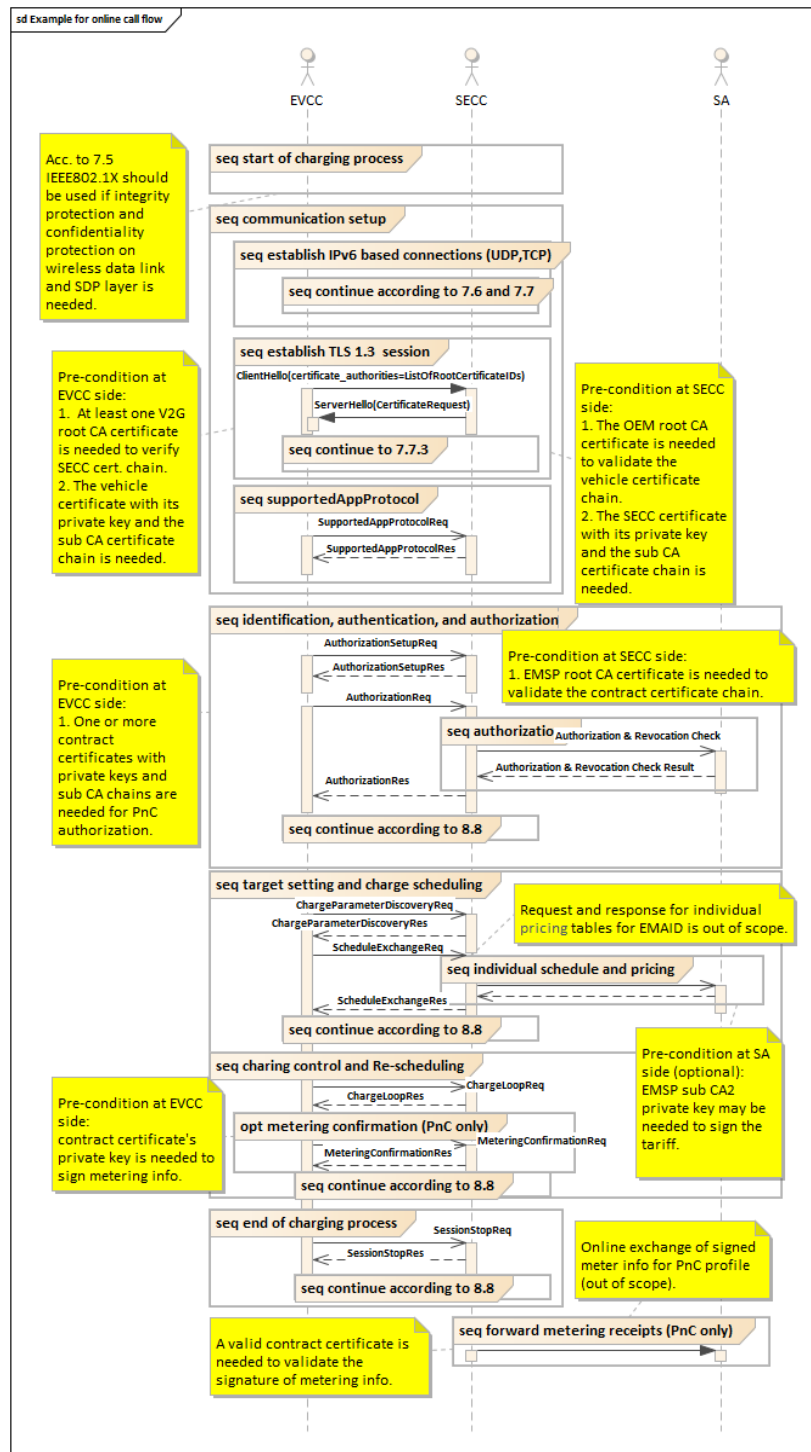


Figure 4 — Example for call flows

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

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

7.3.2 Certificate and key management

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

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

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

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

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

Table 1 — Basic certificate fields

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

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

NOTE 2 IETF RFC 5280 has been updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399. These updates are considered to be included in this document.

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

Table 2 — Certificate extension examples

Certificate extensions	Description
Key usage	Usage of the corresponding private key (e.g. Digital Signature, non-repudiation, key encipherment, ...)
Extended Key Usage	Further specification of key usage using OIDs, e.g.: – server authentication (1.3.6.1.5.5.7.3.1); – client authentication (1.3.6.1.5.5.7.3.2). NOTE Sometimes the following values are encoded here: – 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 can also use strong cryptography for the connection with the client's browser. This extension was used at the time of strong crypto export control to enable financial web site to provide appropriate protection of the data transfer.
CRL distribution point	Location to retrieve certificate revocation lists
OCSP	Location to retrieve OCSP. Refer to IETF RFC 6960 as updated by IETF RFC 8954 for details.
Authority information	Additional authorization information
Subject alternative name	Alternative names of the entity
Basic constraint = CA	True if the certificate is a root certificate or a sub-CA certificate.
subjectAltPublicKeyInfo	Alternative/secondary certificate key data. This contains the alternative key algorithm and the alternative key generated using the said algorithm. Refer to ITU-T X.509 for further details.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NOTE 9 Annex B provides the certificate profiles.

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

NOTE 10 Where necessary, deviations have been specified.

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

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

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

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

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

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

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

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

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

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

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

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

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

NOTE 18 A cross certificate adds one more level.

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

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

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

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

NOTE 20 The certificate validation includes checking the following.

- a) The content of a leaf certificate has not been altered after issue. This means it is possible to check and confirm the signature up to the trust anchor level and thus the integrity of the signed content.
- b) The signature up to the trust anchor level is not compromised (none of the certificates have been revoked). Certificate revocation is checked via the OCSP response (or CRL, if allowed for that particular certificate) as detailed in 7.7.3.1 and 7.7.3.3.
- c) The validity period of each certificate in the chain up to the trust anchor has not yet elapsed.
- d) Each certificate in the certificate chain matches the appropriate certificate profile as defined in Annex B. This includes checking the following:
 - the key length of each certificate in the certificate chain matches the key length specified by that certificate's profile in Annex B;
 - every critical KeyUsage attribute is set to the appropriate value (i.e. 0 or 1) as defined for that certificate's profile in Annex B;

- every mandatory parameter, as defined for that certificate's profile in Annex B, exists;
 - all BasicConstraints attributes are set as defined for that certificate's profile in Annex B;
 - DomainComponent value matches the definition of that certificate's profile in Annex B;
 - the subjectID of the leaf certificate is acceptable [e.g. if the CN (common name) of the certificate is accepted by the V2G entity];
 - the subjectID of the leaf certificate is acceptable [e.g. if the CN (common name) of the certificate is accepted by the V2G entity].
- e) All critical parameters are processed.
- f) All non-critical parameters that are recognized by the relying party are processed.

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

NOTE 22 IETF RFC 5280 has been updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399. These updates are considered to be included in this document.

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

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

7.3.2.1 Certificate structure

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

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

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

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

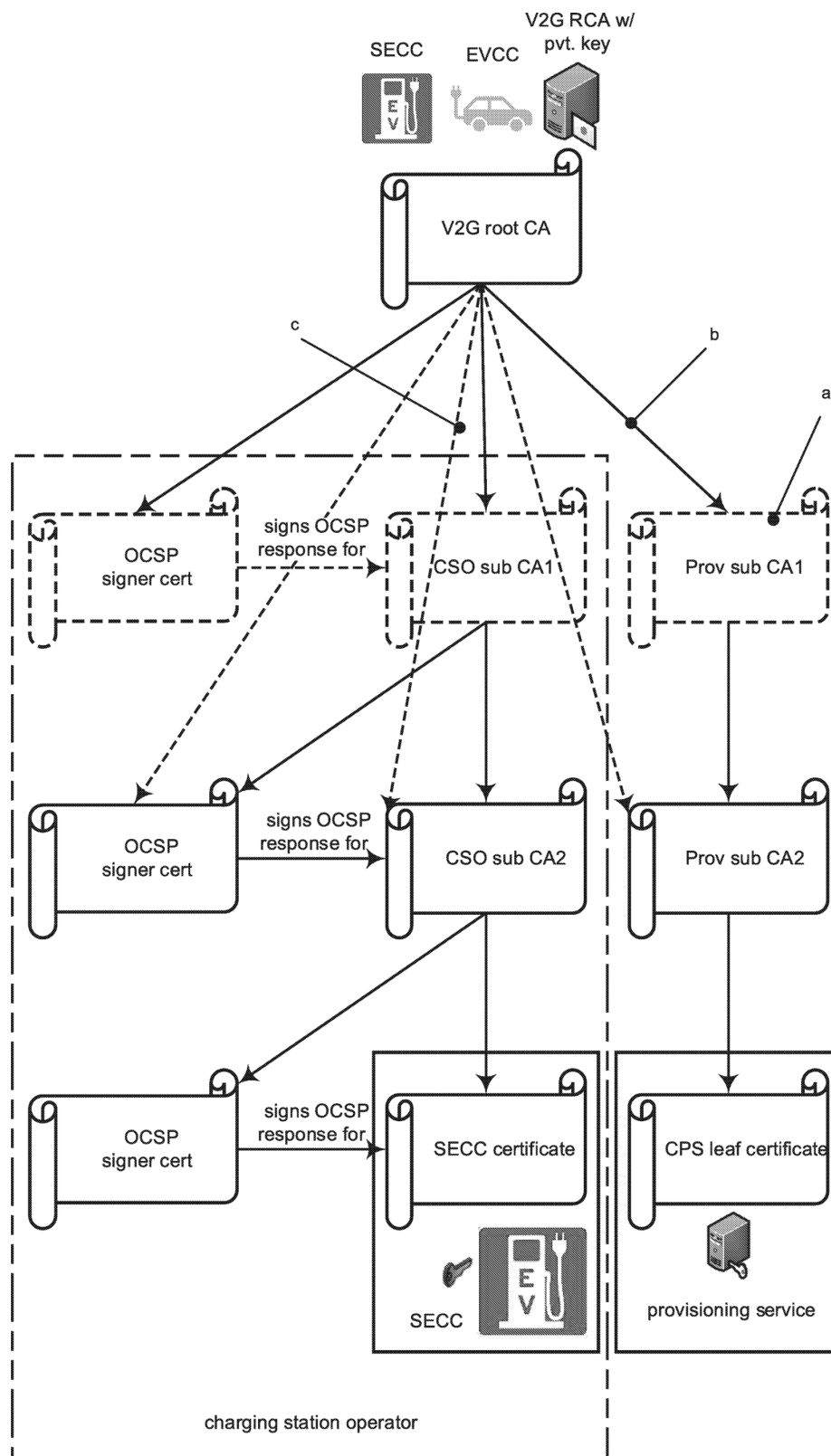
NOTE 2 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the CSO's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use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

[V2G20-2327] An OCSP signer certificate used to sign the OCSP response for SECC certificate status shall be generated using a certificate chain that uses a V2G root CA certificate as the trust anchor. Refer to Figure 5 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of a certificate structure. Refer to Annex B for details of the certificate profile.

NOTE 3 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the CSO's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use as the trust anchor for the OCSP signer certificate that signs the OCSP response for their SECC certificates.

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

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



Key

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

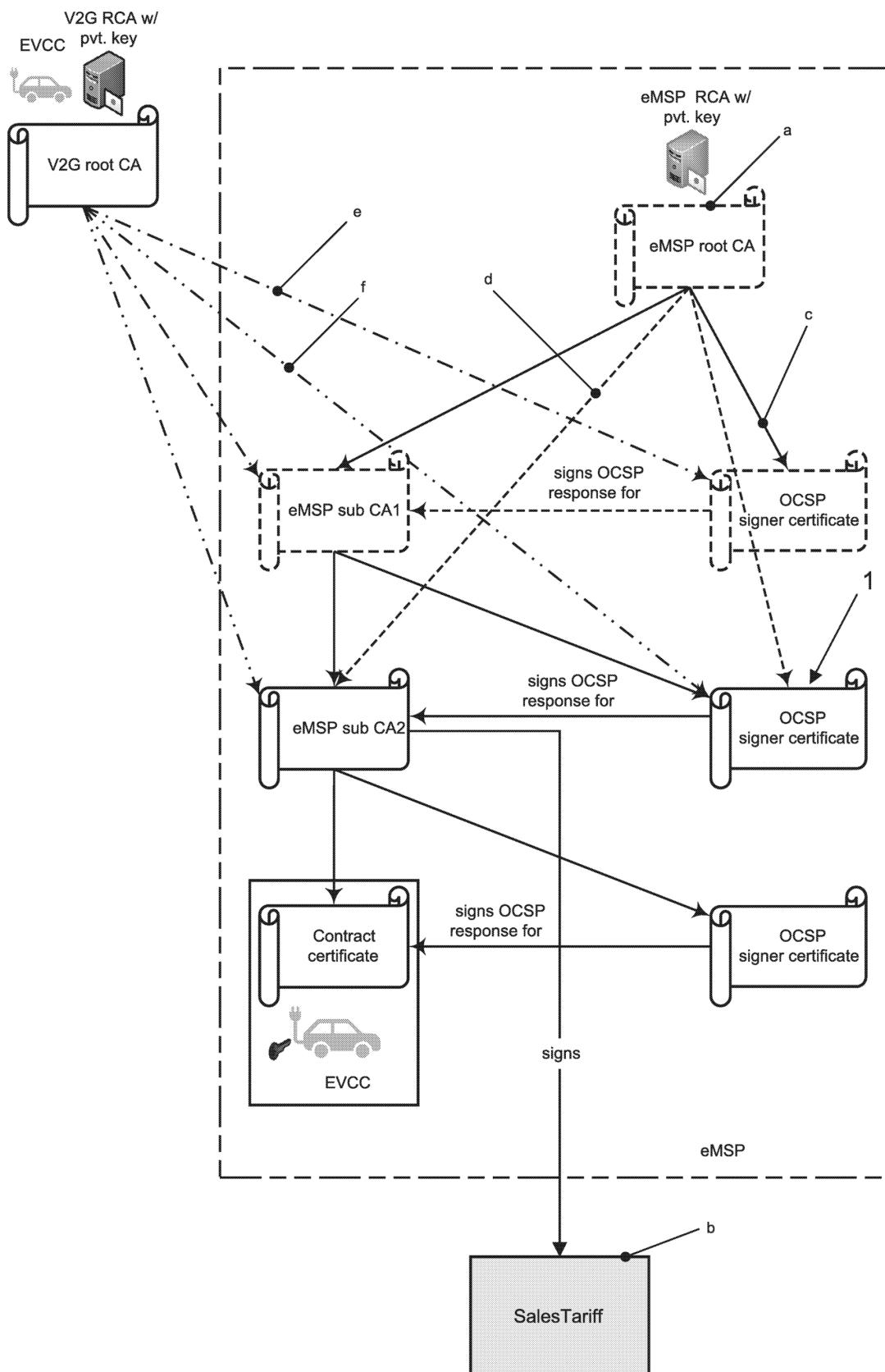
Figure 5 — Mandatory certificate structure originating from V2G root CA certificate

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

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

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

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



Key

1 certificate

a Optional certificate — If the sub-CA1 is not present, the sub-CA2 is signed by the V2G root CA.

- b SalesTariff is not a certificate. The black arrow does not depict a certificate signing or certificate derivation/origination. SalesTariff is data that is signed by the eMSP using the private key of the eMSP sub-CA2. Since, in a PnC use case, the EVCC always contains the eMSP sub-CA2 as part of its contract certificate chain, the EVCC always has the associated public key for eMSP sub-CA2 that it can use to verify the signatures on SalesTariff.
- c Direct certification — The use of sub-CA1 is optional.
- d Optional direct certification — If the sub-CA1 is present, it signs the sub-CA2 certificates.
- e Upon eMSP's discretion the contract certificate chain may originate from V2G root CA certificate. This type of arrow shows when the sub-CA1 is signed by the V2G root CA.
- f Upon eMSP's discretion the contract certificate chain may originate from V2G root CA certificate. This type of arrow shows when the sub-CA1 is not used and sub-CA2 is signed by the V2G root CA.

Figure 6 — Contract certificate structure

[V2G20-2331] A vehicle certificate shall be generated using a certificate chain that uses either an OEM root CA certificate or a V2G root CA certificate as the trust anchor. Refer to Figure 7 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of certificate structure. Refer to Annex B for details of the certificate profile.

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

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

[V2G20-2332] The OCSP signer certificate used to sign the OCSP response for vehicle certificate status shall be generated using a certificate chain that uses either an OEM root CA certificate or a V2G root CA certificate as the trust anchor. Refer to Figure 7 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of certificate structure. Refer to Annex B for details of the certificate profile.

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

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

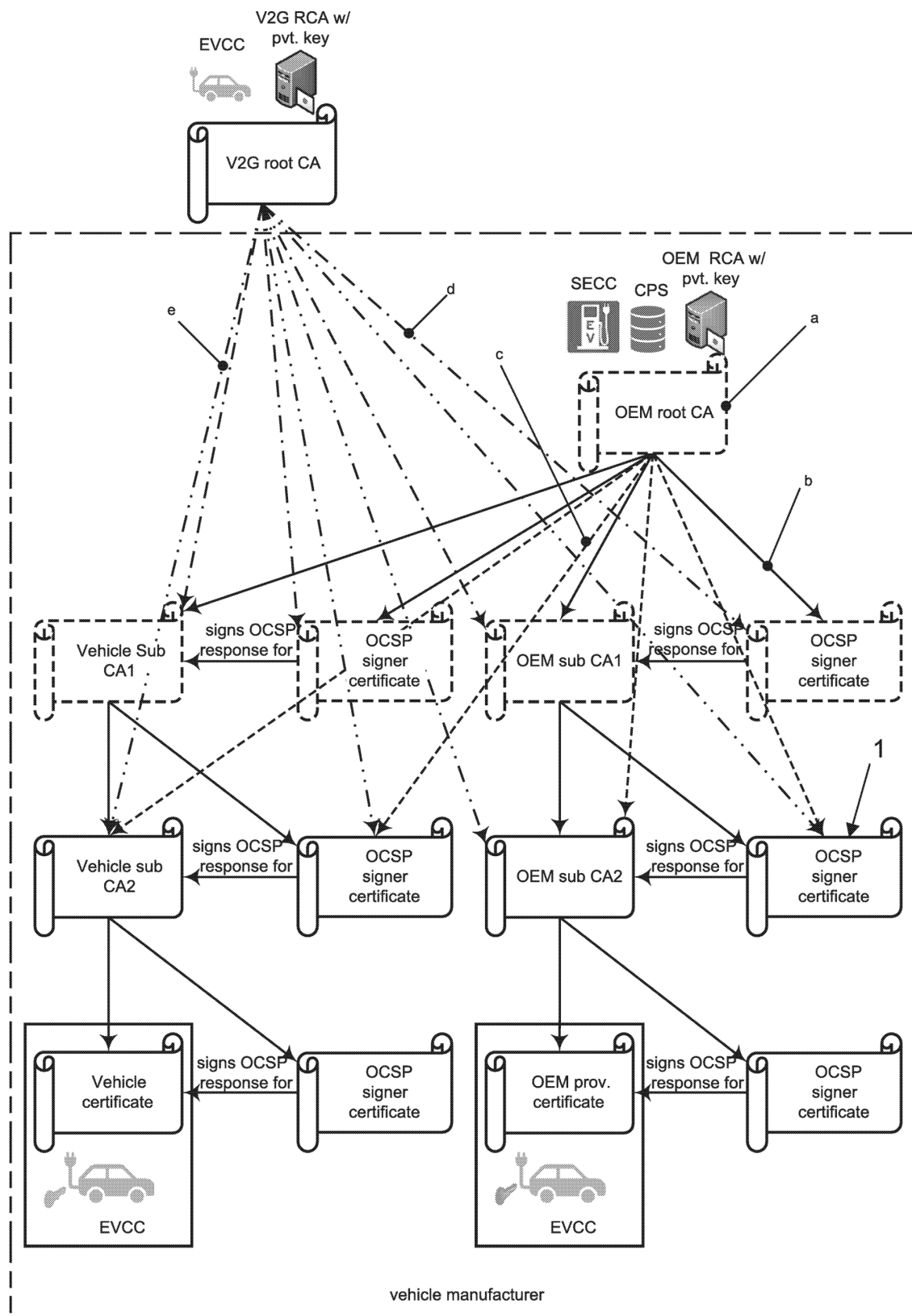
[V2G20-2333] An OEM provisioning certificate shall be generated using a certificate chain that uses either an OEM root CA certificate or a V2G root CA certificate as the trust anchor. Refer to Figure 7 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of certificate structure. Refer to Annex B for details of the certificate profile.

NOTE 11 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the OEM's discretion (while being aware of the applicable

local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use (if any) as the trust anchor for their OEM provisioning certificates.

[V2G20-2334] The OCSP signer certificate used to sign the OCSP response for OEM provisioning certificate status shall be generated using a certificate chain that uses either an OEM root CA certificate or a V2G root CA certificate as the trust anchor. Refer to Figure 7 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of certificate structure. Refer to Annex B for details of the certificate profile.

NOTE 12 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the OEM's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use (if any) as the trust anchor for the OCSP signer certificate that signs the OCSP response for their OEM provisioning certificates.



Key

1 certificate

a Optional certificate — If the sub-CA1 is not present, the sub-CA2 is signed by the V2G root CA.

b Direct certification — The use of sub-CA1 is optional.

c Optional direct certification — If the sub-CA1 is present, it signs the sub-CA2 certificates.

- ^d Upon OEM's discretion the vehicle certificate and OEM provisioning certificate chain may originate from V2G root CA certificate. This type of arrow shows when the sub-CA1 is signed by the V2G root CA.
- ^e Upon OEM's discretion the vehicle certificate and OEM provisioning certificate chain may originate from V2G root CA certificate. This type of arrow shows when the sub-CA1 is not used and sub-CA2 is signed by the V2G root CA.

Figure 7 — Certificate structure originating from OEM root CA certificate

- [V2G20-2335]** A PE certificate shall be generated using a certificate chain that uses a PE private root CA certificate as the trust anchor. Refer to Annex H for further details. Refer to H.1.6 for examples of certificate structure. Refer to Annex B for details of the certificate profile.
- [V2G20-2336]** A PE certificate chain shall not be signed or cross-signed by any CA under a V2G root CA or an eMSP root CA or an OEM root CA. Similarly, PE certificate chain shall not be signed or cross-signed by any V2G root CA or eMSP root CA or OEM root CA.

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

7.3.2.1.1 Minimum required/mandatory certificates

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

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

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

- [V2G20-2338]** Each SECC shall possess at least one of either of the following root certificates:
- V2G root CA certificate;
- OR**
- OEM root CA certificate.

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

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

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

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

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

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

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

NOTE 7 The EVCC can possess more than one V2G root CA certificates.

7.3.2.1.2 Certificates required for PnC

Support for PnC is not mandatory for EVCC/SECC. It is up to the OEM/CSO to decide whether to support PnC or not. If the EVCC wants to support PnC, requirements defined in this subclause are mandatory.

[V2G20-2341] The EVCC shall contain at least one contract certificate or, in case the EVCC supports contract certificate installation via EVSE, storage space for at least one contract certificate. This certificate is necessary for PnC authorization. Refer to 7.3.2.1 for contract certificate requirements.

NOTE 1 EVCC can contain more than one contract certificate.

NOTE 2 This requirement does not provide details of how the contract certificate was installed. This document provides a methodology to install these certificates via EVSE but the OEM can choose to install contract certificates in another manner as suitable for their design.

7.3.2.1.3 Certificates required for installation of contract certificates via EVSE

Support for contract certificate installation via EVSE is not mandatory. It is up to the OEM to decide whether to support contract certificate installation via EVSE or not. If the EVCC wants to support contract certificate installation via EVSE, requirements defined in this subclause are mandatory.

[V2G20-2342] The EVCC shall contain one OEM provisioning certificate. This certificate is necessary for contract certificate installation via EVSE. Refer to 7.3.2.1 for OEM provisioning certificate requirements.

NOTE If the EVCC does not want to install contract certificates via EVSE, this requirement can be skipped.

[V2G20-2343] If the EVCC does not contain an OEM provisioning certificate, it shall not send CertificateInstallationReq message. Refer to 8.3.4.3.9.2 for details of CertificateInstallationReq message. Refer to 7.9.2.5 and its subclauses for details of contract certificate installation via the EVSE.

7.3.2.1.4 Minimum certificates required for PE

This subclause covers both the SECC and the private SECC.

[V2G20-2344] The SECC shall not contain any PE private root CA certificates.

NOTE 1 The SECC is assumed to always operate in public environment.

[V2G20-2345] The SECC operating in public environment shall not contain any PE certificate.

NOTE 2 The SECC is assumed to always operate in public environment.

[V2G20-2346] The private SECC shall not contain any SECC certificate.

[V2G20-2347] The private SECC shall possess a PE private root CA certificate. This certificate is necessary to establish a TLS session. Refer to 7.3.2.1 for PE private root CA certificate requirements.

[V2G20-2348] The private SECC shall contain a PE certificate. This certificate is necessary to establish a TLS session. Refer to 7.3.2.1 for PE certificate requirements.

7.3.2.2 Certificate governance

Certificate governance and lifecycle management is a major aspect of any PKI system to secure the PKI, build trust and provide the necessary assurance. However, these aspects of the PKI system are outside the scope of this document.

A certificate, in and of itself, does not provide assurance on how the certificate holder ensures that the private key associated with the certificate is not compromised, what is the guarantee that the holder of the certificate is actually who they say they are, steps the CA will take when a private key is compromised, etc. That assurance and trust in the certificates comes through a certificate policy, certification practice statement, etc. certificate policy (CP) and certification practice statement (CPS) contain the topics as defined IETF RFC 3647.

X.509 defines a CP as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements".

Per IETF RFC 3647, "When a certification authority (CA) issues a certificate, it is providing a statement to a certificate user (i.e. relying party) that a particular public key is bound to a particular entity (i.e. certificate subject). The extent to which the certificate user should rely on that statement needs to be assessed by the certificate user." The certificate policy provides the information that can be used by a certificate user to decide whether or not to trust a certificate.

Certificate policies are also used to establish trust relationships between CAs (i.e. cross certification). When CAs issue cross certificates, one CA assesses and recognizes one or more certificate policies of the other CA.

Mostly the CAs post the CP, CPS, audit results, etc. publicly so that the certificate users can see how the CA ensures the security of the keys, identity of the certificate holders, manages the certificate lifecycle, etc. and develop trust in the CA.

[V2G20-2349] Any certificates originating from, or cross-signed by, a V2G root CA certificate chain or eMSP root CA certificate chain or OEM root CA certificate chain shall follow a well-established certificate governance structure, including but not limited to CP, CPS, etc.

[V2G20-2350] Any certificates originating from a PE private root CA certificate chain are not required to follow [V2G20-2349] if the private SECC using them is not scheduled to support PnC.

NOTE This does not mean that a governance structure cannot be used in PE. This just says it is not mandated.

[V2G20-2351] Any certificates originating from a PE private root CA certificate chain are required to follow [V2G20-2349] if the private SECC using them is scheduled to support PnC utilizing contract certificates.

This document does not provide any certificate governance structure. With many industry participants, this document leaves it to those participants, the CAs, PKI implementers, etc. to define the certificate governance structure that best suits their use cases. It is envisioned that the industry will automatically gravitate towards robust and secure CAs who have strong CP/CPS and provide periodic audit results along with verifiable data proving that they actually adhere to their CP/CPS.

7.3.3 Number of root certificates and root validity

This subclause defines requirements for storage space for number of various types of root CA certificates for the SECC and EVCC. This subclause does not mandate actual installation of these various root CA certificates in the SECC or EVCC. It is up to the discretion of the CSOs to decide which root CA certificates they want to install in their SECCs and to the OEMs to decide which root CA certificates they want to install in their EVCCs. For example, an OEM may want to support a specific PE for a certain fleet of vehicles

and as such may install the PE private root CA certificate for that particular PE in the EVCC of the EVs in that fleet but may choose not to install any PE private root CA certificate in EVCC in any other EVs it manufactures.

If the communication should work, some root CA certificates are installed in each SECC and EVCC. Depending on the use case of the EV and/or EVSE, the OEMs/CSOs will need to figure out which root CA certificates they should install in their EVCC/SECC so as to enable that particular use case.

[V2G20-1806] Each EVCC shall provide storage space for at least two V2G root CA certificates.

Storing two V2G root CA certificates is required by [V2G20-1806] to be able to store the currently valid V2G root CA certificate of a specific V2G root CA and additionally the new V2G root CA certificate of that V2G root CA that will be valid after the previous V2G root CA certificate has expired.

[V2G20-2352] Each SECC shall provide storage space for at least two V2G root CA certificates.

NOTE 1 It is not mandatory for SECC to support any V2G root CA certificates. A CSO can decide to only offer ISO 15118-20 communications to those EVs whose vehicle certificate is signed (or cross-signed) by an OEM root CA certificate supported by the CSO's SECC.

Storing two V2G root CA certificates is required by [V2G20-2352] to be able to store the currently valid V2G root CA certificate of a specific V2G root CA and additionally the new V2G root CA certificate of that V2G root CA that will be valid after the previous V2G root CA certificate has expired.

NOTE 2 This requirement does not apply to a private SECC.

There can be multiple V2G root CAs in a given market. [V2G20-1806] and [V2G20-2352] define the minimum number of V2G root CA certificates that need to be supported by EVCC and SECC respectively. Regulatory and market conditions may require EVCC and/or SECC to support more than the minimum number of V2G root CA certificates. For example, it is strongly advised, but not mandated, that the EVCC and SECC support all local/regional V2G root CA certificates. This will improve availability of ISO 15118-20 communications and allow the EV to utilize ISO 15118-20 based communications on any local/regional EVSE.

It is not in the scope of this document to define the maximum number of V2G root CA certificates to be supported by the EVCC and/or SECC. It is left up to the OEM to decide on the maximum number of V2G root CA certificates to be supported by the EVCC. Similarly, it is left up to the CSO to decide on the maximum number of V2G root CA certificates to be supported by the SECC.

Additionally, if the EV drives to a different region, it would need V2G root CA certificates for that region. It is not in the scope of this document to define how the OEM manages that situation. But the OEM is advised to take that into account when designing the EVs.

[V2G20-2353] Each public SECC shall provide storage space for at least two OEM root CA certificates.

NOTE 3 It is not mandatory for a public SECC to support any OEM root CA certificates. A CSO can decide to only offer ISO 15118-20 communications to those EVs whose vehicle certificate is signed (or cross-signed) by a V2G root CA certificate supported by the CSO's SECC.

Storing two OEM root CA certificates is required by [V2G20-2353] to be able to store the currently valid OEM root CA certificate of a specific OEM and additionally the new OEM root CA certificate of that OEM that will be valid after the previous V2G root CA certificate has expired.

[V2G20-2354] Each private SECC shall provide storage space for at least one OEM root CA certificate or V2G root CA certificate.

NOTE 4 A private SECC can contain more than one OEM root CA certificates and/or V2G root CA certificates.

There can be multiple OEMs in a given market. [V2G20-2353] defines the minimum number of OEM root CA certificates that need to be supported by the public SECC. [V2G20-2354] defines the minimum number of OEM root CA certificates that need to be supported by the private SECC. Regulatory and market conditions may require the SECC to support more than the minimum number of OEM root CA certificates. For example, it is strongly advised, but not mandated, that the SECC support all local/regional OEM root CA certificates. This will improve availability of ISO 15118-20 communications and allow the EV to utilize ISO 15118-20 based communications on any local/regional EVSE.

It is not in the scope of this document to define the maximum number of OEM root CA certificates to be supported by the SECC. It is left up to the CSO to decide on the maximum number of OEM root CA certificates to be supported by the SECC.

Additionally, as new EV OEMs startup, there would be a need to add OEM root CA certificates for those new OEMs to the SECCs. It is not in the scope of this document to define how the CSO/PE operator manages that. But the CSO/PE operator is advised to take that into account when designing their systems.

[V2G20-2355] Each EVCC should provide storage space for at least one PE private root CA certificate.

NOTE 5 It is not mandatory for the EV to support private environment.

[V2G20-867] Except in private environment (PE), a root CA shall not issue a leaf certificate.

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

NOTE 7 This applies to all root CAs including V2G root CA, OEM root CA, eMSP root CA, etc. except PE private root CA. A PE private root CA can issue a leaf certificate. Refer to 7.3.4 for further details of PE security.

7.3.4 Support and application of TLS

According to 7.3.2 and 7.3.3, this document requires the following TLS:

- 1) the certificate management defined in 7.3.2;
- 2) the key management defined in 7.3.2;
- 3) the certificate chain structure defined in 7.3.2 and 7.3.3;
- 4) the certificate validity period defined in 7.3.2 and 7.3.3.

[V2G20-1238] In the SDP handshake, when the SECC intends to offer ISO 15118-20 communication, it shall respond to a TLS request by the EVCC with TLS.

[V2G20-1235] V2G-CI-TLS shall always be applied for both the EVCC and SECC, if the chosen ProtocolNamespace is equal to "urn:iso:std:iso:15118:-20".

[V2G20-2646] After the message exchange of supportedAppProtocolReq/Res, usage of V2G-CI-TLS shall be confirmed.

[V2G20-1237] If the established connection between EVCC and SECC is TLS 1.2 (or lower) or TCP without TLS the EVCC shall not offer ISO 15118-20 communication in SupportedAppProtocolReq message (see Table 5).

[V2G20-2356] If the established connection between EVCC and SECC is TLS 1.2 (or lower) or TCP without TLS the SECC shall not select ISO 15118-20 communication from SupportedAppProtocolReq message (see Table 5).

Private environment is considered to be a power transfer service for a closed user group. This user group is defined and managed by the eMSP of the power transfer service itself. The security of the field is

managed according to the security policy of the eMSP, so the authentication of private SECC by EVCC through TLS connection might be negligible. Refer to H.2 for further details of PE security.

7.3.5 Firewall

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

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

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

[V2G20-1013] There shall be at least one firewall between the EVCC, which is connected to an untrusted network, and the SECC, which is connected to a trusted network.

[V2G20-1014] For security reasons the rules mentioned in Table 3 shall apply for the firewall mentioned in [V2G20-1013].

Table 3 — Firewall action for wireless communication

Source		Destination		Protocol	Interface		Action
IP address	Port	IP address	Port		Inbound	Outbound	
all	EVCC Port (dynamic range)	ff02:01	15118	UDP	untrusted	trusted	allow
all	EVCC Port (dynamic range)	SECC IP address	SECC Port (V2G_DST_TCP_DATA)	TCP	untrusted	trusted	allow
all	EVCC Port (dynamic range)	SECC IP address	1080	TCP	untrusted	trusted	allow
SDP server IP address	15118	EVCC IP address	EVCC port	UDP	trusted	untrusted	allow
SECC IP address	SECC Port (V2G_DST_TCP_DATA)	EVCC IP address	EVCC port	TCP	trusted	untrusted	allow
SECC IP address	1080	EVCC IP address	EVCC port	TCP	trusted	untrusted	allow
SECC IP address	SECC Port [SECC_VAS_Port]	EVCC IP address	EVCC port	TCP	trusted	untrusted	allow
all	all	all	all	all	trusted	trusted	allow
all	all	all	all	all	all	all	deny
NOTE "Allow" means to establish a connection and "deny" means port-unreachable for the source.							

7.3.6 Protection of the cryptographic keys

The private keys of certificates are sensitive data. Once a private key gets compromised, it cannot be trusted anymore and therefore not supposed to be used anymore. If one of these private keys could be

read by an attacker, the attacker could impersonate the original equipment. It is considered good security practice that each V2G entity and any PKI operator additionally protects all private keys and symmetric keys. This can range from simple security measures such as setting readout protection fuse bits in the microcontroller to more advanced protection via secure boot facilities, debug access protection, and embedded hardware security modules (HSM). The HSMs offer a high level of security including protection against physical attacks. A suitable HSM provides a secure environment for private key and symmetric key operations. It offers interfaces to use the private key and the symmetric keys but ensures that the keys cannot be read out or manipulated.

The V2G entity or the PKI operator can use a trusted platform module (TPM) 2.0 to implement the HSM.

The TPM 2.0 is representative of a HSM that is qualified for the automotive use cases according to AEC-Q100, has Common Criteria (CC) EAL4+ certification and can implement the desired security features. A TPM 2.0 can securely store sensitive data such as private keys, provides a secure execution environment for symmetric and asymmetric cryptographic operations (including secure random number generation) and enables additional security mechanisms such as the direct import of encrypted keys, credential protection, secured (measured) boot and a policy-based enhanced authorization mechanism. The TPM 2.0 library specification developed by the Trusted Computing Group (TCG) is adopted as open international standards ISO/IEC 11889-1:2015, ISO/IEC 11889-2:2015, ISO/IEC 11889-3:2015 and ISO/IEC 11889-4:2015.

7.3.6.1 Protection of the EVCC keys

In an EVCC environment, the private keys of the contract certificate, vehicle certificate and the OEM provisioning certificate are considered to be sensitive data. The EVCC can protect the private keys and symmetric keys (including session keys) by employing secure environments like HSM that offer interfaces to use the keys but ensures that the keys cannot be read out or manipulated, even from a program running on the EVCC. A customized HSM may even accept input of an encrypted contract certificate private key, so that the private key is never accessible outside of the HSM in plain, unencrypted form. Such a HSM can be integrated into the EVCC as a separate physical package or as an on-chip microcontroller extension.

It is advised that the EVCC keeps the keys secure under all conditions, including while they are in use. An easy way to achieve this is to utilize the HSM to store and use the keys including any cryptographic operations that use those keys.

In addition, the EVCC can also utilize the HSM to perform other cryptographic functions in a secure manner (e.g. encryption/decryption, signature calculation and verification, asymmetric key-pair generation, etc.).

The EVCC can opt to use TPM to perform all (or some) of the functions mentioned above for the HSM. Refer to 7.3.6 for details of TPM.

7.3.6.2 Protection of the keys in public SECC

This subclause does not cover requirements for the private SECC. It only covers requirements for a public SECC. In some cases, though, a private SECC may be required to meet these requirements as well. Such cases will be specifically called out. In a public SECC environment, the private key of the SECC certificate is considered to be sensitive data. It is advised that the public SECC protects the private key and symmetric keys (including session keys) by employing secure environments like HSM that offer interfaces to use the keys but ensure that the keys cannot be read out or manipulated, even from a program running on the public SECC. Such a HSM can be integrated into the public SECC as a separate physical package or as an on-chip microcontroller extension.

It is recommended that the public SECC keeps the keys secure under all conditions, including while they are in use. An easy way to achieve this is to utilize HSM to store and use the keys including any cryptographic operations that use those keys.

In addition, the public SECC can also utilize the HSM to perform other cryptographic functions in a secure manner (e.g. encryption/decryption, signature calculation and verification, asymmetric key-pair generation, etc.).

The public SECC can opt to use TPM to perform all (or some) of the functions mentioned above for the HSM. Refer to 7.3.6 for details of TPM.

7.3.6.3 Protection of the keys in private SECC

This subclause does not cover requirements for the SECC operating in public environment. It only covers requirements for a private SECC. Since the private SECC operates in a private environment, it is not required to follow the same security requirements as an SECC operating in a public environment.

However, to improve security of the solution, private SECC is encouraged to meet the similar security standards as an SECC operating in a public environment. Refer to 7.3.6.2 for further details.

[V2G20-2357] Any private SECC that supports PnC (using contract certificate(s)) shall meet the same security standards as an SECC operating in a public environment. Refer to 7.3.6.2 for further details.

7.3.7 Random number generation

Asymmetric cryptographic algorithms like ECDSA, EdDSA, etc. strongly rely on the fact that an attacker does not have information about the random nonce. Otherwise, signatures would leak information about the secret key. Depending on the type of defect in the random generator implementation, this may enable an attacker to derive the secret key after a certain number of signatures. In the worst case, simple reuse of the random nonce will enable an attacker to calculate the secret key after only two signatures. Therefore, it is vital to have a suitable random number generator (RNG), a so-called cryptographically secure RNG. In addition, for generating the initialization vector in AES-GCM, for generating a challenge for PnC and for generating a nonce for TLS session negotiation a cryptographically secure RNG is needed.

[V2G20-835] Whenever a V2G entity requires random numbers within this document, a state-of-the-art cryptographically secure random number generator shall be used.

NOTE 1 There could already be a suitable, cryptographically secure random number generator available in the implementation. As the actual implementation of the RNG does not affect interoperability, this document does not prescribe a specific way in order to be future-proof and to avoid duplication. Some examples of established RNG standards are NIST SP 800-90 A, German BSI AIS 20/AIS 31, etc.

NOTE 2 Additionally, IETF RFC 8937 provides a few methodologies for improvement of randomness for some use cases.

In general, there are two different kinds of RNGs, a deterministic random bit generator (DRBG) that utilizes an algorithm to produce random numbers based on a seed input. These kinds of RNGs are quite fast in producing a random number but suffer from the consequences of using a seed as an input. These kinds of RNGs have a few advantages like speed, no loss of entropy over time or usage, etc. As such, DRBGs are usually the preferred class of RNGs. These RNGs are also called pseudo-random number generator (PRNG).

Not all DRBGs are cryptographically secure. The random number generated by a DRBG is only as random as the input seed. If the input seed is known, the output random number could be predicted. As such, DRBGs are usually seeded every so often by another kind of RNG called non-deterministic random bit

generator (NRBG) that utilizes unpredictable physical processes/phenomenon to generate the random numbers. These kinds of RNGs do not require a seed as an input, but are much slower at generating the random number as they first gathers enough physical entropy before they can generate a random number. Additionally, these kinds of RNGs tend to loose entropy over time or with usage. Hence, NRBGs are usually not used for direct generation of a random number. In cryptographic applications, they are mostly used to seed a DRBG. These RNGs are also called true-random number generator (TRNG).

[V2G20-2607] The V2G entity shall ensure that the random number used to re-seed/re-initialize a DRBG has the minimum amount of entropy required for the particular application/feature/function as defined by this specification document. The entropy input and the seed shall be kept secret.

NOTE 3 Some applications could accept a low amount of entropy in the random number while others could require a very high amount of entropy. It is left up to the different applications/features/functions to define the amount of entropy needed for those particular applications/features/functions.

NOTE 4 As mentioned earlier, NRBGs can take some time to build entropy. If the seed for the DRBG is generated by a NRBG, there can be a need to either wait for the NRBG to build enough entropy before requesting the NRBG to generate the random number (seed) or the random number could be generated and securely stored at a time when the NRBG is known to have a good entropy and using that random number to re-seed/re-initialize the DRBG when the need to re-seed/re-initialize the DRBG arrives/occurs.

[V2G20-2608] The V2G entity shall keep a random number generated according to [V2G20-835] secret and shall use this random number only once.

7.3.7.1 Random number generator best practices

Cryptographic algorithms are highly dependent on random numbers. An implementation of the security architecture defined by this document is only as secure as the RNG implemented by the V2G entity and secure usage of the random numbers generated by that RNG.

Random number produced by a RNG should be used/processed securely.

If the V2G entity stores the random number generated by NRBG before using it, it should ensure security of that stored random number, such that no processes other than the process that actually needs to use the random number, have access to that random number. Similarly, the V2G entity should ensure that the seed (number generated by NRBG used to re-seed DRBG) is erased from memory after it has been used to re-seed the DRBG.

If the V2G entity uses a DRBG to generate the random number and the DRBG is seeded using a NRBG, the DRBG should be re-seeded/re-initialized from the NRBG at least once every 24 h or at power-up, whichever occurs earlier.

Most cryptographic RBGs are advertised as being able to produce 0,93 bits (or so) of entropy for every 1 bit generated by the RBG. In such cases a 128-bit random number generated by the RBG will have 120 bits of entropy. Requirements below take that into account when defining the minimum entropy requirements.

Higher the entropy, better the RBG is. Most applications/features/functions in this document require minimum 0,90 bits of entropy for every 1 bit generated. That means, they require 116 bits of entropy in a 128-bit random number.

If an application/feature/function in this document does not specify a minimum entropy requirement, it should be assumed to require minimum of 116 bits of entropy for any random number used by that application/feature/function.

NOTE 116 bits of entropy is based on 0,9 bits of entropy/bit generated by the RBG for a 128 bit number.

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 the EVCC and SECC. This document focuses on protocols above the data link layer. The data link layer is described in ISO 15118-3 and ISO 15118-8.

This subclause defines the basic requirements for establishing communication above the data link layer. This 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 8.6 and its subclauses. Figure 8 depicts the general communication states of the V2G communication from an EVCC perspective. The following applies for the EVCC:

- [V2G20-014]** After the 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.
- [V2G20-016]** The EVCC shall process the IP address assignment mechanism as defined in 7.6.3.2 and 7.6.3.3.
- [V2G20-018]** 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.
- [V2G20-019]** The EVCC shall start the SDP client according to 7.10.1.
- [V2G20-1804]** After receiving an SDP response with transport protocol set to TCP and security option set to TLS, the EVCC shall establish the TLS connection to the SECC as described in 7.7.3.
- [V2G20-1805]** If [V2G20-1804] is not fulfilled, then ISO 15118-20 (this document) shall not be offered by the EVCC during SupportedAppProtocolReq or selected by the SECC in SupportedAppProtocolRes. Refer to Table 5 for further details of services/standards that can be supported in such a condition.
- [V2G20-024]** After the TLS connection is established, the EVCC shall initiate the V2G communication session as defined in Clause 8.
- [V2G20-025]** The EVCC shall terminate the TLS connection after stopping the V2G communication session.
- [V2G20-717]** If the EVCC sent the message SessionStopReq with parameter ChargingSession equal to "Terminate" it shall terminate the Data-Link (D-LINK_TERMINATE.request()) after receiving the message SessionStopRes.
- [V2G20-1227]** If the EVCC sent the message SessionStopReq with parameter ChargingSession equal to "Pause" it shall pause the Data-Link (D-LINK_PAUSE.request()) after receiving the message SessionStopRes with ResponseCode set to "OK" and follow the sleep and wake-up requirements defined in ISO 15118-3:2015, 7.6.
- [V2G20-719]** Whenever the EVCC receives the indication for a missing Data-Link (D-LINK_READY.indication(DLINKSTATUS=No link)), the EVCC shall continue with [V2G20-014].

[V2G20-720] If the EVCC identifies any error it shall indicate a Data-Link error (D-LINK_ERROR.request()) and continue with [V2G20-014].

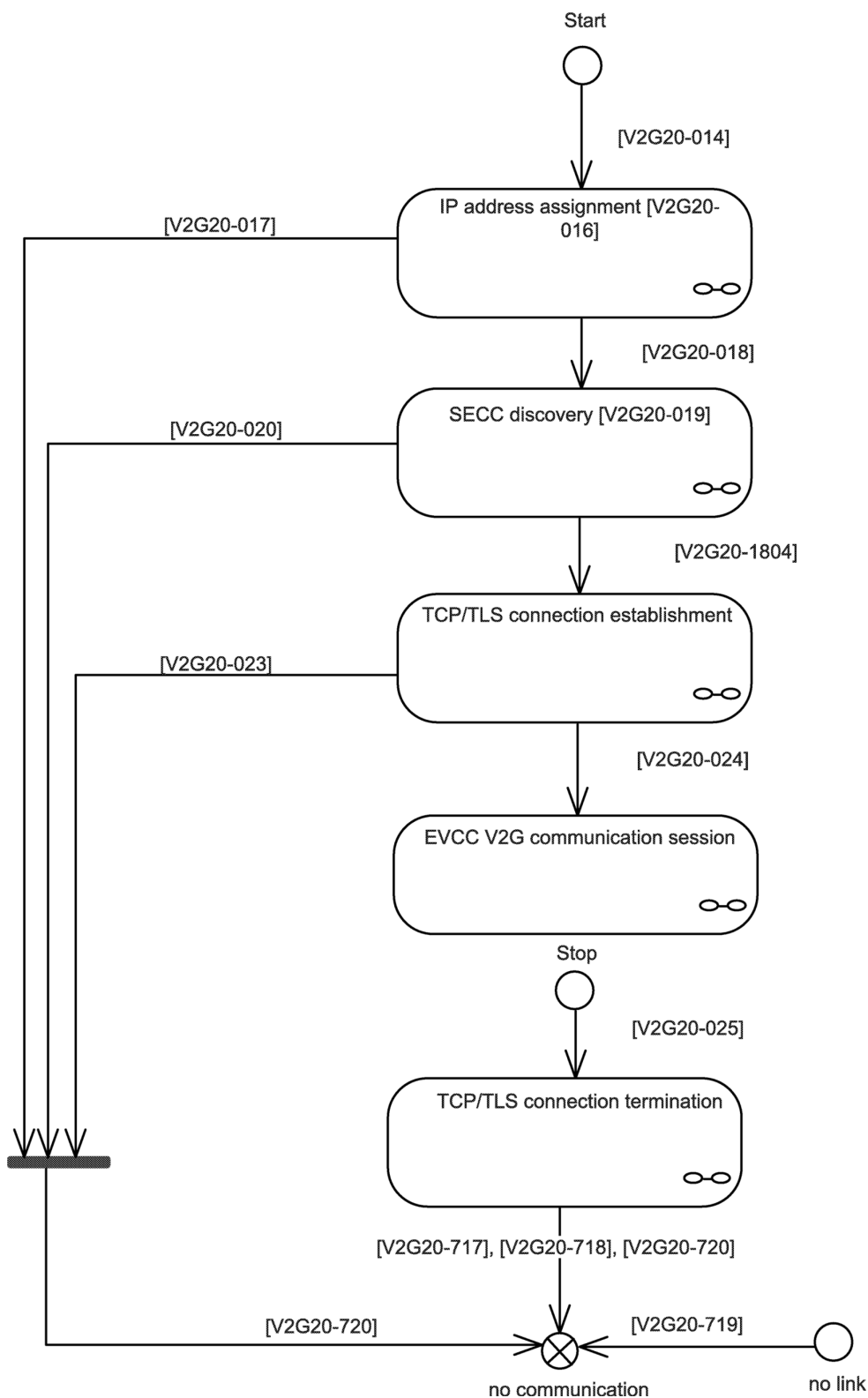


Figure 8 — Overview V2G communication states EVCC

Figure 9 depicts the general communication states of the V2G communication from an SECC perspective. The following applies for the SECC:

[V2G20-721] After indication of a successful Data-Link establishment (D-LINK_READY.indication(DLINKSTATUS=Link established)), the SECC shall initiate the address assignment mechanism.

[V2G20-026] The SECC shall configure an IP address (static or dynamic) by any appropriate mechanism.

NOTE 1 To enable the integration of an SECC in different communication infrastructures, the definition of the address assignment for the SECC is not in the 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, for example, a static IP or the mechanism described in 7.6.3.2 and 7.6.3.3.

[V2G20-027] After the IP address is assigned, the SECC shall start the SDP server as defined in 7.10.1.

NOTE 2 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.

[V2G20-723] The SECC may stop the SDP server when SECC_CommunicationSetup_Timer is equal or larger than V2G_SECC_CommunicationSetup_Performance_Time.

[V2G20-029] The SECC may stop the IP address assignment mechanism when V2G_SECC_CommunicationSetup_Timer is equal or larger than V2G_SECC_CommunicationSetup_Performance_Time.

[V2G20-030] After the SDP server is started successfully, the SECC shall wait for a TLS connection initialization depending on the SDP response message as defined in 7.10.1.6.

[V2G20-031] The SECC shall wait until the TLS connection is established.

[V2G20-032] The SECC shall stop waiting for establishing the TLS connection when V2G_SECC_CommunicationSetup_Timer is equal or larger than V2G_SECC_CommunicationSetup_Performance_Time.

[V2G20-033] After the TLS connection is established, the SECC shall wait for the initialization of the V2G communication session as defined in Clause 8.

[V2G20-722] If [V2G20-033] applies the SECC may stop the SDP server after successful establishment of a TLS connection.

[V2G20-034] The SECC shall terminate the TLS connection after stopping the V2G communication session.

[V2G20-1776] If the SECC received the message SessionStopReq with parameter ChargingSession equal to "Terminate" it shall terminate the Data-Link (D-LINK_TERMINATE.request()) 2 s after sending the message SessionStopRes.

[V2G20-1777] If the SECC received the message SessionStopReq with parameter ChargingSession equal to "Pause" it shall pause the Data-Link (D-LINK_PAUSE.request()) after sending the message SessionStopRes with ResponseCode set to "OK" and follow the sleep and wake-up requirements defined in ISO 15118-3:2015, 7.6.

[V2G20-726] Whenever the SECC receives the indication for a missing Data-Link (D-LINK_READY.indication(DLINKSTATUS=No link)), the SECC shall continue with [V2G20-721].