BS EN ISO 15118-2:2016

BSI Standards Publication

Road vehicles — Vehicle-to-Grid Communication Interface

Part 2: Network and application protocol requirements (ISO 15118-2:2014)

Documents
Document Sharing Hub

Full document details: BS EN ISO 15118-2:2016

National foreword

This British Standard is the UK implementation of EN ISO 15118-2:2016. It is identical to ISO 15118-2:2014. It supersedes BS ISO 15118-2:2014 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee PEL/69, Electric vehicles.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2016.
Published by BSI Standards Limited 2016

ISBN 978 0 580 90930 6

ICS 43.120

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2014.

Amendments issued since publication

Date	Text affected
31 May 2016	This corrigendum renumbers BS ISO 15118-2:2014 as BS EN ISO 15118-2:2016.

Documents
Document Sharing Hub

Full document details: BS EN ISO 15118-2:2016

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 15118-2

April 2016

ICS 43.120

English Version

Road vehicles - Vehicle-to-grid communication Interface - Part 2: Network and application protocol requirements (ISO 15118-2:2014)

Véhicules routiers - Interface de communication entre véhicule et réseau électrique - Partie 2: Exigences du protocole d'application et du réseau (ISO 15118-2:2014)

Straßenfahrzeuge - Kommunikationsschnittstelle zwischen Fahrzeug und Ladestation - Teil 2: Anforderungen an das Netzwerk- und Anwendungsprotokoll (ISO 15118-2:2014)

This European Standard was approved by CEN on 21 February 2016.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

© 2016 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. EN ISO 15118-2:2016 E

Documents
Document Sharing Hub

Full document details: BS EN ISO 15118-2:2016

European foreword

The text of ISO 15118-2:2014 has been prepared by Technical Committee ISO/TC 22 “Road vehicles” of the International Organization for Standardization (ISO) and has been taken over as EN ISO 15118-2:2016 by Technical Committee CEN/TC 301 “Road vehicles” the secretariat of which is held by AFNOR.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by October 2016, and conflicting national standards shall be withdrawn at the latest by October 2016.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 15118-2:2014 has been approved by CEN as EN ISO 15118-2:2016 without any modification.

Documents
Document Sharing Hub

Full document details: BS EN ISO 15118-2:2016

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 3

4 Symbols and abbreviated terms 7

5 Conventions 8
5.1 Definition of OSI based services 8
5.2 Requirement structure 8
5.3 Usage of RFC references 8
5.4 Notation used for XML schema diagrams 9

6 Document overview 9

7 Basic requirements for V2G communication 11
7.1 General information 11
7.2 Service primitive concept of OSI layered architecture 11
7.3 Security concept 12
7.4 V2G communication states and data link handling 21
7.5 Data Link Layer 26
7.6 Network Layer 26
7.7 Transport Layer 28
7.8 V2G Transfer Protocol 32
7.9 Presentation Layer 36
7.10 Application Layer 46

8 Application Layer messages 55
8.1 General information and definitions 55
8.2 Protocol handshake definition 56
8.3 V2G Message Definition 60
8.4 V2G Communication Session and BodyElement Definitions 62
8.5 Complex data types 104
8.6 Identification Modes and Message Set definitions 137
8.7 V2G communication timing 170
8.8 Message sequencing and error handling 184
8.9 Request-Response Message Sequence examples 206

Annex A (informative) Mapping of Part 1 use case elements 214

Annex B (informative) Mapping of ISO 15118 message element names to SAE J2847/2 terms 250

Annex C (normative) Schema definition 254

Annex D (informative) Message examples 278

Annex E (informative) Application of certificates 299

Annex F (normative) Certificate profiles 313

Annex G (informative) Encryption for the Distribution of Secret Keys 321

Annex H (normative) Specification of Identifiers 323

Annex I (informative) Message sequencing for renegotiation 326

Annex J (informative) Overview on XML Signatures 330

Documents
Document Sharing Hub

© ISO 2014 – All rights reserved

Full document details: BS EN ISO 15118-2:2016

Annex K (informative) Summary of requirements **334**
Bibliography **341**

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

Foreword

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

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

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

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 22, *Road vehicles*, Subcommittee SC 3, *Electrical and electronic equipment*.

ISO 15118-2 was developed in conjunction with IEC TC 69, *Electric road vehicles and electric industrial trucks*.

ISO 15118 consists of the following parts, under the general title *Road vehicles — Vehicle-to-Grid Communication Interface*:

— *Part 1: General information and use-case definition*

— *Part 2: Network and application protocol requirements*

— *Part 3: Physical and data link layer requirements*[1]

[1] To be published.

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

Introduction

The pending energy crisis and necessity to reduce greenhouse gas emissions has led the vehicle manufacturers to a very significant effort to reduce the energy consumption of their vehicles. They are presently developing vehicles partly or completely propelled by electric energy. Those vehicles will reduce the dependency on oil, improve the global energy efficiency and reduce the total CO_2 emissions for road transportation if the electricity is produced from renewable sources. To charge the batteries of such vehicles, specific charging infra-structure is required.

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

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

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

INTERNATIONAL STANDARD **ISO 15118-2:2014(E)**

Road vehicles — Vehicle-to-Grid Communication Interface — Part 2: Network and application protocol requirements

1 Scope

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

The purpose of this part of ISO 15118 is to detail the communication between an EV (BEV or a PHEV) and an EVSE. Aspects are specified to detect a vehicle in a communication network and enable an Internet Protocol (IP) based communication between EVCC and SECC.

Key

1 Scope of ISO/IEC FDIS 15118-2:2013(E)

2 Message definition considers use cases defined for communication between SECC to SA

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

This part of ISO 15118 defines messages, data model, XML/EXI based data representation format, usage of V2GTP, TLS, TCP and IPv6. In addition, it describes how data link layer services can be accessed from a layer 3 perspective. The Data Link Layer and Physical Layer functionality is described in ISO 15118-3.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 3166-1, *Codes for the representation of names of countries and their subdivisions — Part 1: Country codes*

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

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

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

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

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

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IETF RFC 5095, *Deprecation of Type 0 Routing Headers in IPv6 (December 2007)*

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

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

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

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

IETF RFC 5289, *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM) (August 2008)*

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

IETF RFC 5722, *Handling of Overlapping IPv6 Fragments (December 2009)*

IETF RFC 6066, *Transport Layer Security (TLS) Extensions: Extension Definitions (January 2011)*

IETF RFC 6106, *IPv6 Router Advertisement Options for DNS Configuration (November 2010)*

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

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS EN ISO 15118-2:2016

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

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

NIST Special Publication 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised) (March 2007)

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

3 Terms and definitions

For the purposes of this document, the terms in ISO 15118-1 and the following apply.

3.1
Basic Charging
BC
charging phase during a charging session controlled by IEC 61851-1 only

3.2
charging limits
set of physical constraints (e.g. voltage, current, energy, power) that is negotiated during a V2G Communication Session for a charging session

3.3
Communication Setup Timer
Timer monitoring the time from plug-in until the Session Setup message

3.4
Contract Certificate
certificate issued to EVCC either by V2G Root CA or by Sub-CA, which is used in XML Signatures in application layer so that SECC or secondary actor can verify the Contract issued to the EVCC and signatures issued by the EVCC

3.5
CP State
Control Pilot (Vehicle) State according to IEC 61851-1 signalled on Control Pilot Line

3.6
credentials
anything that provides the basis for confidence, belief, credit, etc.

EXAMPLE Examples include certificates, passwords, user names etc.

3.7
Data Link Setup
setup phase for establishing the data link

Note 1 to entry: Entry Condition: Any valid control pilot signal according to IEC 61851-1; Exit Condition: D-LINK_READY.indication(DLINKSTATUS=LinkEstablished).

3.8
Distinguished Encoding Rules = ASN-1 encoding rule
DER
method for encoding a data object, such as an X.509 certificate, to be digitally signed or to have its signature verified

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

3.9
global address
IP address with unlimited scope

3.10
High Level Communication Charging
HLC-C
charging phase during a charging session controlled by ISO 15118

3.11
link-local address
IP address with link-only scope that can be used to reach neighbouring interfaces attached to the same link

3.12
Identification Mode
mandatory and optional messages and parameters with respect to charging scenarios using External Identification Means (EIM) and charging scenarios using Plug and Charge (PnC) for identification

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

3.13
(IP) address
IP-layer identifier for an interface or a set of interfaces

3.14
Maximum Transfer Unit
MTU
maximum size (in bytes) of the largest protocol data unit that the Data Link Layer that can be pass onwards

3.15
Message Set
set of mandatory V2G messages and parameters for the EVCC or SECC covering one or multiple use case elements

3.16
Message Timer
Timer monitoring the exchange of a Request-Response-Pair

3.17
network segment
collection of devices that can exchange data on Data Link Layer level directly via Data Link Addresses

EXAMPLE Ethernet: all devices which can see each other via MAC addresses.

3.18
node
device that implements IPv6

3.19
OEM Provisioning Certificate
certificate issued to the EVCC, so that a Contract Certificate can be securely requested and received from a secondary actor

3.20
Performance Time
non-functional timing requirement defining the time a V2G Entity shall not exceed when executing or processing certain functionality

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

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

3.21
private environment
area with (physical) access limited to a small number of vehicles (EVs), which may be a private parking garage or a garage / parking lot of a company with its own EV fleet, where one or several private wall-box(es) are used instead of public charging stations as EVSE, and where in order to keep the private wall-box simple and cheap in production and operation it is allowed to stay offline permanently, which allows a private wall-box to use leaf certificates with a longer maximum validity than allowed for public charging stations and using a private root certificate which is different to the V2G root certificates and which has to be installed into each EV that is allowed to charge within this specific private environment, resulting in a limited number of EVs belonging to one private environment, the difference to a “trusted environment” being that in a (pure; i.e. not additionally “trusted”) private environment TLS and the corresponding data encryption at connection level is always used, and solely certificate handling is simplified for the private wall-box (EVSE) since it may stay offline permanently, resulting in unrestricted certificate validity periods, shorter certificate chain length, omitting OCSP, and an additional “pairing mode”

3.22
Identification Mode
group of mandatory and optional Message Sets covering a set of similar charging scenarios for a specific identification means

3.23
renegotiation
messaging for updating the agreement on the charging schedule between EV and EVSE during a V2G Communication Session by retransmitting the parameters SASchedule and ChargingProfile

3.24
Request-Response Message Pair
request message and the corresponding response message

3.25
Request-Response Message Sequence
predefined sequence of Request-Response Message Pairs

3.26
SDP Client
V2G Entity that uses the SDP server to get configuration information about the SECC to be able to access the SECC

3.27
SDP Server
V2G Entity providing configuration information for accessing the SECC

3.28
SECC Certificate
certificate issued to SECC either by V2G Root CA or by Sub-CA, which is used in TLS so that the EVCC can verify the authenticity of the SECC

3.29
Sequence Timer
Timer monitoring a Request-Response Message Sequence

3.30
Sub-CA
subordinate certificate authority who issues SECC Certificates and/or Contract Certificates on behalf of the V2G Root CA

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

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

3.31
Sub-CA Certificate
certificate issued to Sub-CA

3.32
TCP_DATA
socket/interface for data transfer based on TCP connection

3.33
Timeout
timing requirement defining the time a V2G Entity monitors the communication system for a certain event to occur

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

3.34
Timer
device or piece of software used in an implementation for measuring time.

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

3.35
Trusted Environment
closed user group (e. g. members of car sharing system) with some pre-distributed token for access to the SECC charging service (e.g. key to home garage, RFID token for car sharing), which is something where a person or instance is responsible for, for example (not limited to) a person with its home garage, a car sharing operator or a taxi operator

3.36
V2G Charging Loop
V2G messaging phase for controlling the charging process by ISO 15118

3.37
V2G Communication Session
association of two specific V2G Entities for exchanging V2G messages

3.38
V2G Entity
primary actor participating in the V2G communication using a mandatory or optional transmission protocol defined by ISO 15118-2

3.39
V2G Message
message exchanged on application layer

Note 1 to entry: Refer to Clause 8 Application Layer messages.

3.40
V2G Setup
setup phase for V2G messaging

Note 1 to entry: Entry Condition: D-LINK_READY.indication(DLINKSTATUS=LinkEstablished); Exit Condition: PowerDeliveryReq with ChargeProgress equals Start or Stop.

3.41
V2G Transfer Protocol
communication protocol to transfer V2G messages between two V2GTP entities

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

3.42
V2GTP Entity
V2G Entity supporting the V2G Transfer Protocol

3.43
V2G Root CA
certificate Authority (CA) who issues Contract Certificates and/or SECC Certificates, or who delegates ability to issue such Certificates to Sub-CA

3.44
V2G Root Certificate
certificate issued to V2G Root CA

4 Symbols and abbreviated terms

For the purposes of this document, the following abbreviated terms apply:

BEV	Battery Electric Vehicle
CA	Certificate Authority
CRL	Certificate Revocation List
DH	Diffie Hellman
DER	Distinguished Encoding Rules
ECDSA	Elliptic Curve Digital Signature Algorithm
EMAID	E-Mobility Account Identifier
EMOCH	E-Mobility Operator Clearing House (see also 15118-1, [12])
EV	Electric Vehicle
EVCC	Electric Vehicle Communication Controller
EVSE	Electric Vehicle Supply Equipment
EXI	Efficient XML Interchange
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
NACK	Negative Acknowledgement
PDU	Protocol Data Unit
PHEV	Plug-in Hybrid Electric Vehicle
PKI	Public Key Infrastructure
PLC	Power Line Communication
PnC	Plug and Charge
SA	secondary actor

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

SDP	SECC Discovery Protocol
SDU	Service Data Unit
SECC	Supply Equipment Communication Controller
TCP	Transmission Control Protocol
V2G	Vehicle to Grid Communication
V2G CI	Vehicle-to-Grid Communication Interface
V2GTP	V2G Transfer Protocol
UDP	User Datagram Protocol
XML	Extensible Markup Language

5 Conventions

5.1 Definition of OSI based services

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

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

5.2 Requirement structure

This document uses a requirement structure i.e. a unique number identifies each individual requirement included in this document. This requirement structure allows for easier requirement tracking and test case specification. The following format is used:

"[V2G"Y"-"XXX"]" requirement text Where:

— **"**V2G**"** represents the ISO 15118 set of standards,

— Y represents the document part of the ISO 15118 document set

— XXX represents the individual requirement number and

— "requirement text" includes the actual text of the requirement.

EXAMPLE **[V2G2-000]** This shall be an example requirement.

5.3 Usage of RFC references

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

[V2G2-001] In this document, if a referenced RFC has been updated by one or several RFC, the update is fully applicable.

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

[V2G2-003] All published Errata, for the ISO 15118 referenced RFCs, are fully applicable in this standard.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

5.4 Notation used for XML schema diagrams

This standard makes use of XML as a description format for V2G messages. For details with regards to the XML schema diagram notation used in this document refer to Altova XMLSpy Manual.

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

— complex type use capitalized first letters

— simple types use non capitalized first letters

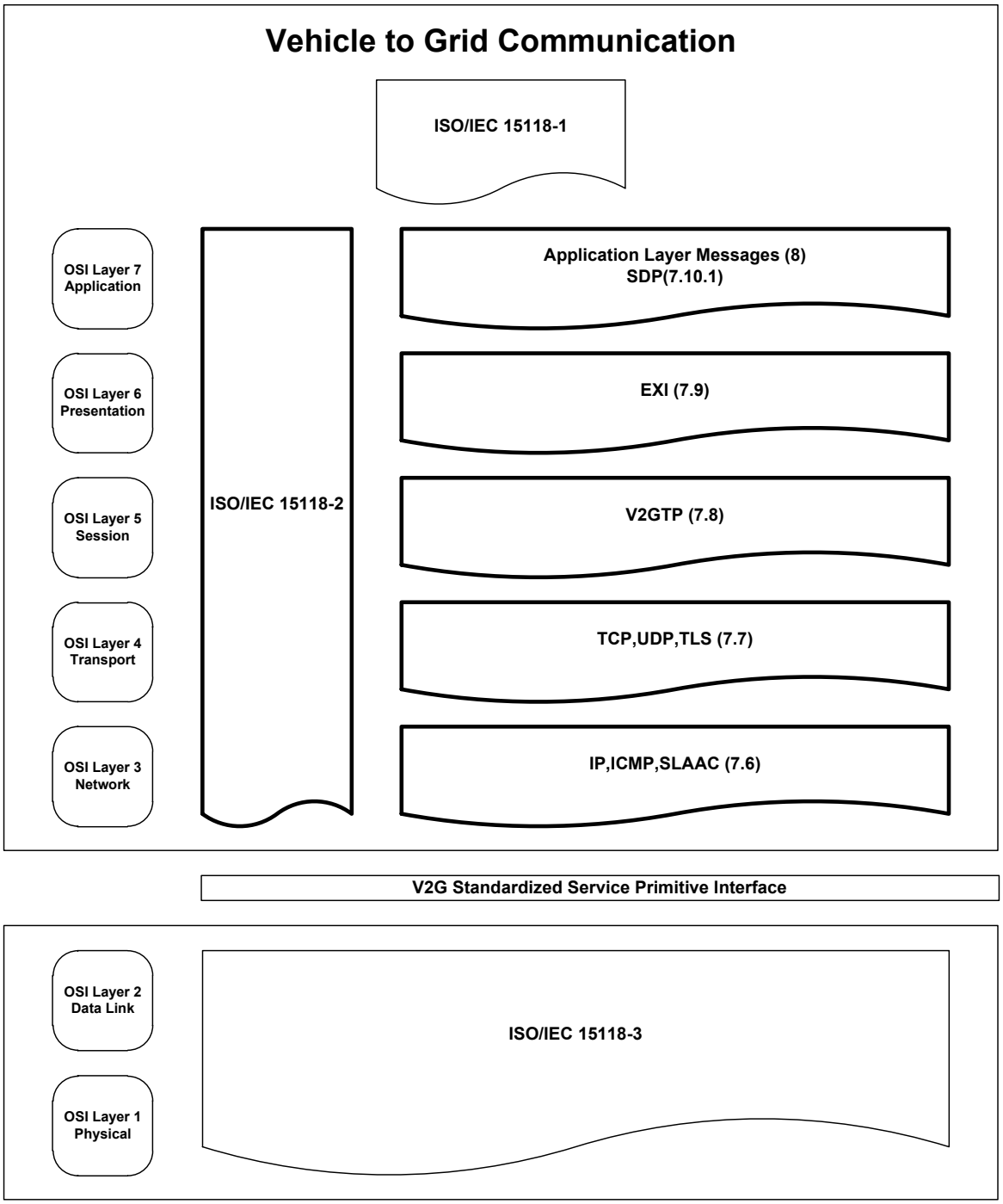
6 Document overview

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

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

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016



Key

OSI Layers and applicable requirements described in this Part of ISO 15118

OSI Layers and applicable requirements defined in other Parts of ISO 15118

Figure 2 — Vehicle to Grid Communication document overview

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

7 Basic requirements for V2G communication

7.1 General information

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

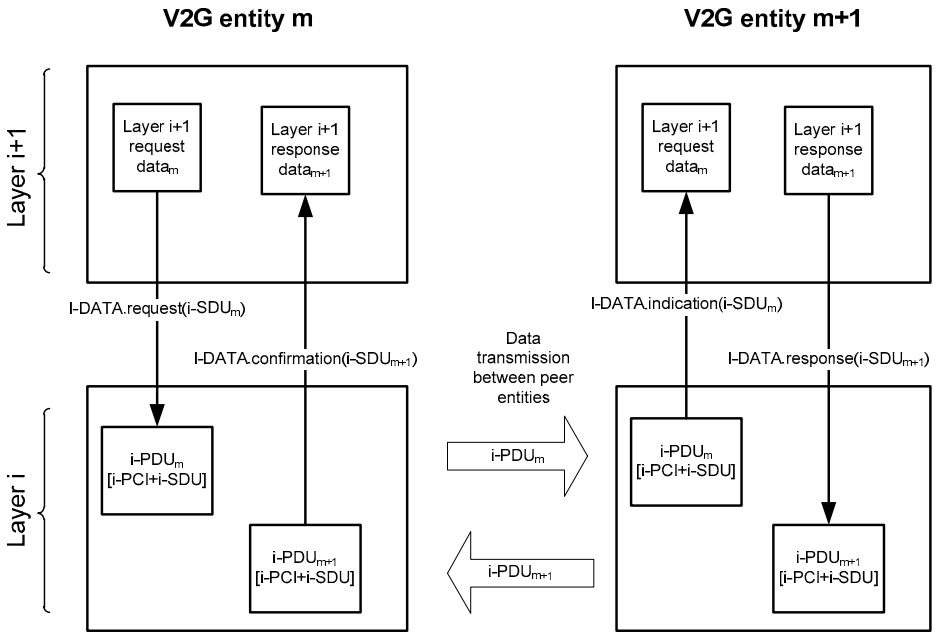
7.2 Service primitive concept of OSI layered architecture

7.2.1 Overview

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

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

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



Key

PDUX: 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.

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

7.2.2 Syntax of service primitives

Service primitives are described with the following syntax:

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

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

— whereas [NAME] is the name of the primitive

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

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

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

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

7.3 Security concept

7.3.1 Call Flows (Flow Charts)

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

The full data flow / sequence charts can be found in subclause 8.8 of this document. In these overview figures only the security relevant information shall be highlighted.

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

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

In this Plug-and-Charge example, all TCP/IP based communication is protected using a unilaterally authenticated TLS channel between the two peers. (Note: TLS is not mandatory for certain Identification Modes other than the Plug-and-Charge Identification Mode). All communication is terminated at the SECC. The meter reading is cyclically signed by the vehicle to support the billing process (refer to 8.4.3.13.1). This information may be used for billing if local regulations permit it. The EVSE provides the charging records, containing the signed meter reading to the backend for further processing.

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

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

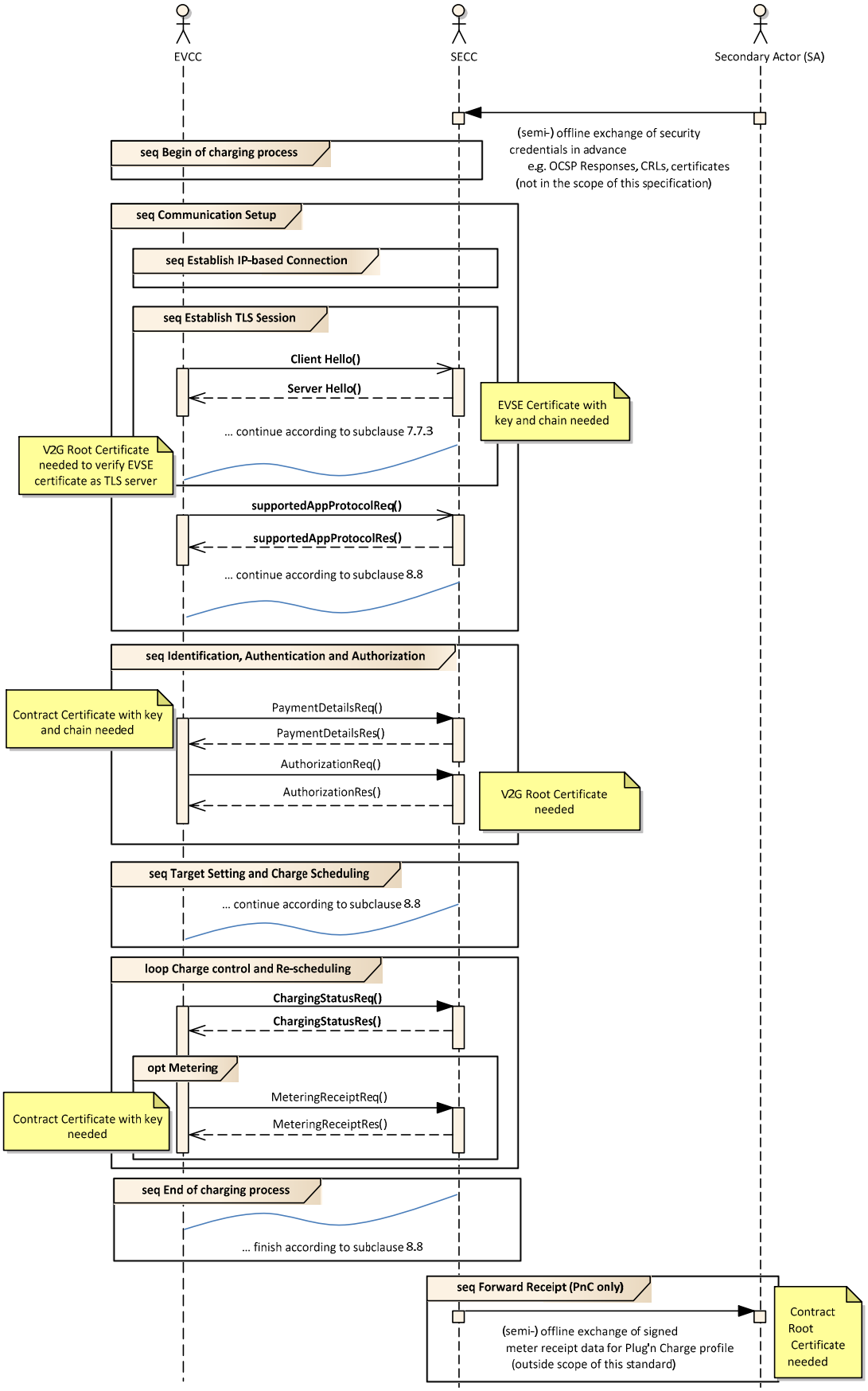


Figure 4 — Example for semi-online communication (1 of 2)

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

Figure 5 shows an example for an online Plug and Charge use case:

As in the semi-online case, in this Plug-and-Charge example, all TCP/IP based communication is protected using a unilaterally authenticated TLS channel between the two peers. (Note: TLS is not mandatory for certain Identification Modes other than the Plug-and-Charge Identification Mode). Some of the information provided by the vehicle may need to be sent to the SA for further processing, like the eMAID or the vehicles credentials to be able so sign the tariff information. The EVCC calculates a charging profile (refer to subclause 8.4.3.9.2) and sends it to the SECC. The SECC may send it to SA systems like Smart Grid or Demand Clearing House. The further process is similar to the semi-online case with the exception, that the final charging data can be directly submitted to the SA. It is assumed that the SECC will also use a secure transport connection to the SA, although the security of the vehicle communication to the SA is secured on application layer.

NOTE 2 The communication between SECC and SA in Figure 5 is shown for informational purpose only and not intended to specify a particular message sequence.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

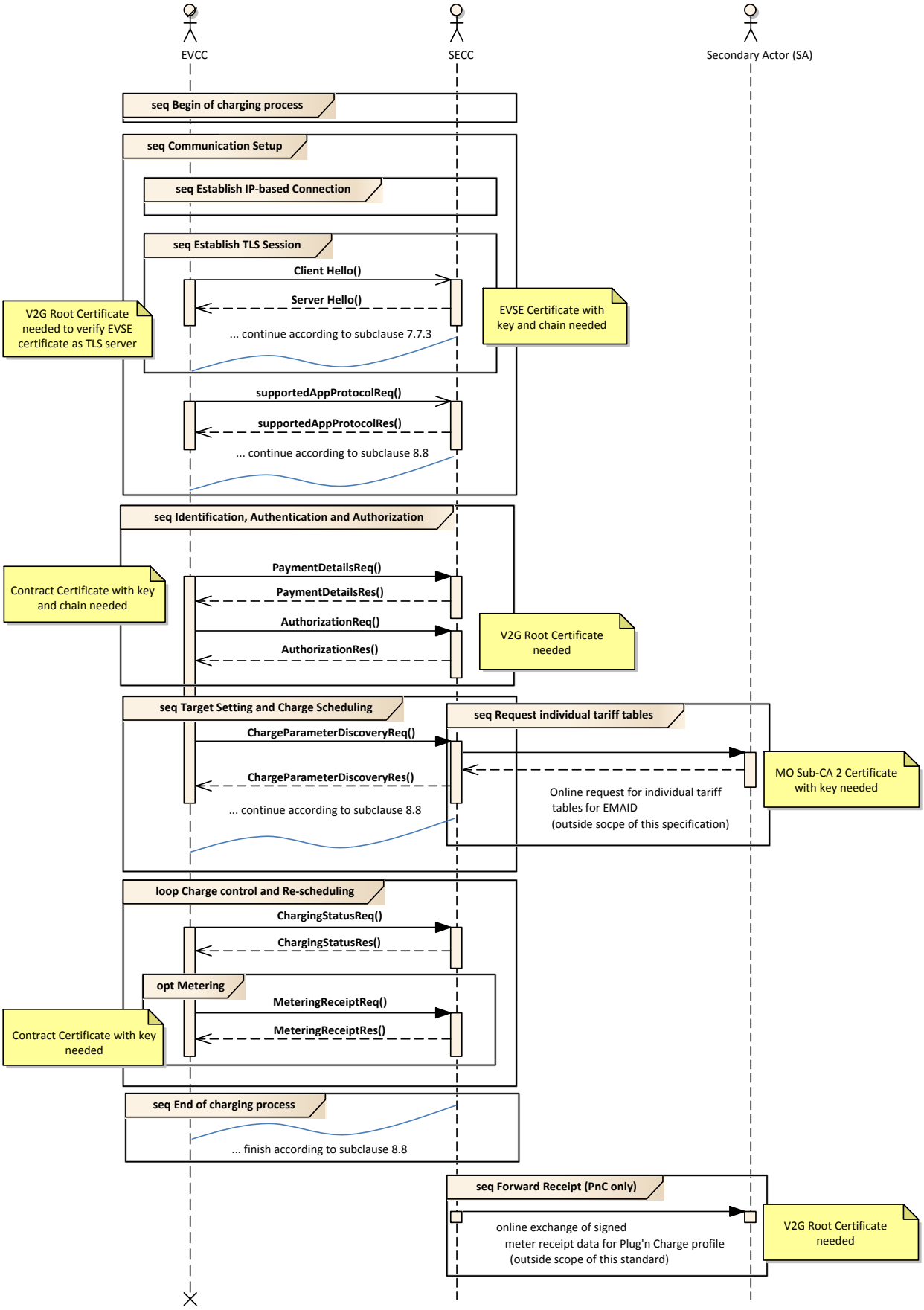


Figure 5 — Example for online communication

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

There are further use cases where security mechanism are needed on application layer. These are the initial enrolment of contract keys and certificate as well as the update of the certificate. In this case vehicle specific OEM keys are used. Those mechanisms are described in Annex 0. An overview on all needed certificates can be found in Annex F.

7.3.2 Certificate and key management

The call flows shown in subclause 7.3.1 require the existence of multiple certificates to be applied for the different security layers. There are SECC Certificates used in the TLS layer for EVCC to authenticate SECC. There are Contract Certificates used at the application layer to authenticate against an SECC and/or secondary actor. There are V2G Root Certificates and possibly Sub-CA Certificates which certify SECC Certificates and Contract Certificates.

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

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

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

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

Table 1 — Basic Certificate Fields

Certificate field	Description
Version	Version of certificate (for 15118 shall be v3 = 0x2)
Serial number	Unique number of certificate (within the domain of the issuer)
Signature algorithm	Used signature algorithm
Issuer	Entity, who has issued and signed the certificate
Validity period	Time period, in which the certificate is valid
Subject	Entity, to which the certificate is issued
Public key	Public key corresponding to a private key
Issuer UID	Optional issuer unique identifier
Subject UID	Optional subject unique identifier
Extensions	Optional (see Table 2)
Signature	Signature of the certificate generated by the issuer

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

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

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

Table 2 — Certificate extension examples

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

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

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

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

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

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

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

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

[V2G2-910] The EVCC should implement a mechanism to check the validity periods of certificates and OCSP responses.

[V2G2-886] The EVCC may choose the accuracy of its time source at its own discretion, but it shall respect the chosen accuracy when using the time source. The accuracy should be at least one day.

NOTE 3 This requirement theoretically even allows for precisions of e.g. one year. The implementer should carefully weigh the security consequences of such a decision.

NOTE 4 If a TLS connection is built up successfully, the EVCC might use the time from a EVSETimeStamp field sent from the SECC through said connection for synchronization of its internal clock, however the implementer should carefully weigh the security consequences of such a decision.

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

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

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

[V2G2-008] Each EVCC shall support at least one V2G Root Certificate.

[V2G2-877] Each SECC shall support the storage of at least 10 V2G Root Certificates.

NOTE 1 Due to overlapping validity periods, up to 10 concurrently valid certificates may exist. See V2G2-012

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

NOTE 3 It is assumed that the V2G Root Certificates applied on OSI layer 4 are also used on OSI layer 7. Additionally it is assumed that in Europe there will be a single root certificate authority similar to the Trust Center that was established for the EURO5/EU5. It is also assumed that other regions of the world will also manage to have a root certificate authority covering a greater number of actors. This leads to the assumption that 5 root certificates for 5 world-regions are sufficient. If one decides for more space for certificates this doesn't affect compatibility. For the SECC however it is mandatory to store more since there might be 10 root certificates valid concurrently for each world-region.

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

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

[V2G2-010] The size of a certificate in DER encoded form shall be not bigger than 800 Bytes. For transmission, all certificates shall be DER encoded.

[V2G2-011] The validity period of any V2G Root Certificate shall be 40 years.

[V2G2-012] At any point in time there shall be a V2G Root Certificate available which is valid for each V2G Root CA at least the next 35 years.

NOTE 5 For explanations of certificate validity, number of root certificates, certificate depth and size refer to Annex E.1.

[V2G2-878] The maximum number of concurrently valid V2G Root Certificates for one Root CA shall be never more than 10.

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

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

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

[V2G2-911] If only one Sub-CA layer is used, i.e. a Sub-CA signed by a Root CA directly signs leaf certificates, the profile of Sub-CA 2 shall apply for that Sub-CA.

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

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

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

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

[V2G2-883] The validity times of SECC Certificates having a trusted Private Operator Root Certificate as their trust anchor may be chosen by the certificate signer at his own discretion.

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

NOTE 7 That means, a Private Operator Root Certificate directly signs a leaf certificate.

7.3.4 Support and Application of TLS

[V2G2-630] Support of TLS is mandatory for the EVCC for all Identification Modes except for Identification Mode "EIM" with Message Set EIM charging AC and Message Set EIM charging DC, in both cases excluding Message Set VAS as defined in subclause 8.6.

[V2G2-631] Support of TLS is mandatory for the SECC for all Identification Modes except for Identification Mode "EIM" in a Trusted Environment with Message Set EIM charging AC and Message Set EIM charging DC, in both cases excluding Message Set VAS as defined in subclause 8.6.

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

[V2G2-632] If a V2G Communication Session without TLS is used, the SECC shall only provide the EIM Identification Mode and the Message Sets EIM charging AC or EIM charging DC by indicating "ExternalPayment" in the parameter PaymentOptionList of the ServiceDiscoveryRes message as defined in subclause 8.4.3.3.3.

[V2G2-633] If a V2G Communication Session without TLS is used, the EVCC shall only accept the EIM Identification Mode with Message Sets EIM charging AC or EIM charging DC, no matter if the SECC offers also other Identification Modes and Message Sets.

[V2G2-634] If a V2G Communication Session without TLS is used, the SECC shall not provide the PnC Message Sets.

[V2G2-635] If a V2G Communication Session without TLS is used, the EVCC shall not apply the PnC Message Sets.

[V2G2-636] If a V2G Communication Session without TLS is used, the SECC shall not provide the Message Set VAS.

[V2G2-637] If a V2G Communication Session without TLS is used, the EVCC shall not apply the Message Set VAS.

[V2G2-638] Security measures for Value Added Services enabled by the Message Set VAS (offered in ServiceDiscoveryRes) are out of scope of this standard.

[V2G2-639] If TLS is not applied both sides have to ensure that an Identification Mode change from EIM to another Identification Mode and a Message Set change from EIM AC or EIM DC to another Message Set in the current charging session is not possible (avoiding security downgrade of the changed to session).

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

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

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

Table 3 — TLS implementation / support for EIM Identification Modes

	Other Environment (not trusted)				Trusted Environment [c]			
Allowed Message Sets [a]	**DC EIM**	**AC EIM**	**DC EIM, VAS**	**AC EIM, VAS**	**DC EIM**	**AC EIM**	**DC EIM, VAS**	**AC EIM, VAS**
EVCC TLS support	optional	optional	mandatory	mandatory	optional	optional	mandatory	mandatory
SECC TLS support	mandatory	mandatory	mandatory	mandatory	optional	optional	mandatory	mandatory
TLS usage negotiation using SDP [b]	EV decides, EVSE shall accept EVs decision	EV decides, EVSE shall accept EVs decision	EV shall use TLS, EVSE shall reject, if EV uses no TLS	EV shall use TLS, EVSE shall reject, if EV uses no TLS	refer to Table 4	refer to Table 4	EV shall use TLS, EVSE shall reject, if EV uses no TLS	EV shall use TLS, EVSE shall reject, if EV uses no TLS

[a] This refers to messages as defined in this standard. In case of VAS, of course any other connections (which are not part of this standard) are possible

[b] Rejecting means to stop communication

[c] See Section 3 for a definition

NOTE 8 Not supporting TLS in the SECC might lead in general to aborted charging sessions with particular EVs as it is in the responsibility of the EV to accept sessions without TLS.

Table 4 — SDP handshake with AC and DC EIM Identification Mode in trusted environment

EVCC TLS support	SECC TLS support	SDP request by EVCC	SDP response SECC
EVCC has TLS support	SECC has TLS support	EVCC signals TLS	SECC shall respond TLS
		EVCC signals TCP	SECC shall respond TCP
	SECC has no TLS support	EVCC signals TLS	SECC can indicate that it does no support TLS with indicating "0x10 = No transport layer security" in its SDP response. The EV can decide, if it wants to establish TCP without TLS, or otherwise stop the communication setup.
		EVCC signals TCP	SECC shall respond TCP
EVCC has no TLS support	SECC has TLS support	EVCC signals TCP	SECC shall respond TCP
	SECC has no TLS support	EVCC signals TCP	SECC shall respond TCP

NOTE 9 For the Message Set "EIM AC" and "EIM DC" it is in the responsibility of the EV to decide on not using TLS and accepting the risk of an unsecured connection.

NOTE 10 If TLS is applied, it is always used with unilateral (EVSE-side) authentication. If TLS is not used, there is no EVSE side authentication towards the EV as well as further protection of the communication channel on transport layer.

NOTE 11 Any functional safety related risks occurring through overvoltage and overcurrent (accidental or purposeful) need to be addressed by implementing the related electrical safety standards (e.g. IEC 61851 and ISO 17409)

Any functional safety related risks occurring through overvoltage and overcurrent are to be handled according requirements listed below:

[V2G2-643] The EVSE shall support the safety measures described in IEC 61851-1 and IEC 61851-22 to protect against overvoltage and overcurrent when using the AC EIM Identification Mode

[V2G2-644] The EVSE shall support the safety measures described in IEC 61851-1 and IEC CDV 61851-23 to protect against overvoltage and overcurrent when using the DC EIM Identification Mode.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

7.4 V2G communication states and data link handling

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

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

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

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

The following applies for the EVCC:

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

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

[V2G2-017] The EVCC shall stop the IP address assignment mechanism as defined in subclauses 7.6.3.2 and 7.6.3.3 when V2G_EVCC_CommunicationSetup_Timer is equal or larger than V2G_EVCC_CommunicationSetup_Timeout.

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

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

[V2G2-645] Depending on the requested security and transport protocol in the SDP request message and the awaited security and transport protocol sent by SDP server, the EV shall decide on the application of TLS.

[V2G2-020] The EVCC shall stop the SDP when V2G_EVCC_CommunicationSetup_Timer is equal or larger than V2G_EVCC_CommunicationSetup_Timeout.

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

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

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

[V2G2-023] The EVCC shall stop to attempt to establish a TLS or TCP connection when V2G_EVCC_CommunicationSetup_Timer is equal or larger than V2G_EVCC_CommunicationSetup_Timeout.

[V2G2-024] After the TLS or TCP connection is established, the EVCC shall initiate the V2G Communication Session as defined in clause 8.

[V2G2-025] The EVCC shall terminate the TLS or TCP connection after stopping the V2G Communication Session.

AVA Documents
Document Sharing Hub

© ISO 2014 – All rights reserved

Full document details: BS EN ISO 15118-2:2016

[V2G2-717] If the EVCC sent the message SessionStopReq with parameter ChargingSession equal to "Terminate" it shall terminate the Data-Link (D-LINK_TERMINATE.request()) after receiving the message SessionStopRes.

[V2G2-718] If the EVCC sent the message SessionStopReq with parameter ChargingSession equal to "Pause" it shall pause the Data-Link (D-LINK_PAUSE.request()) after receiving the message SessionStopRes and continue with **[V2G2-014]**.

[V2G2-719] Whenever the EVCC receives the indication for a missing Data-Link (D-LINK_READY.indication (DLINKSTATUS=No link), the EVCC shall continue with **[V2G2-014]**.

[V2G2-720] If the EVCC identifies any error it shall indicate an Data-Link error (D-LINK_ERROR.request()) and continue with **[V2G2-014]**.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

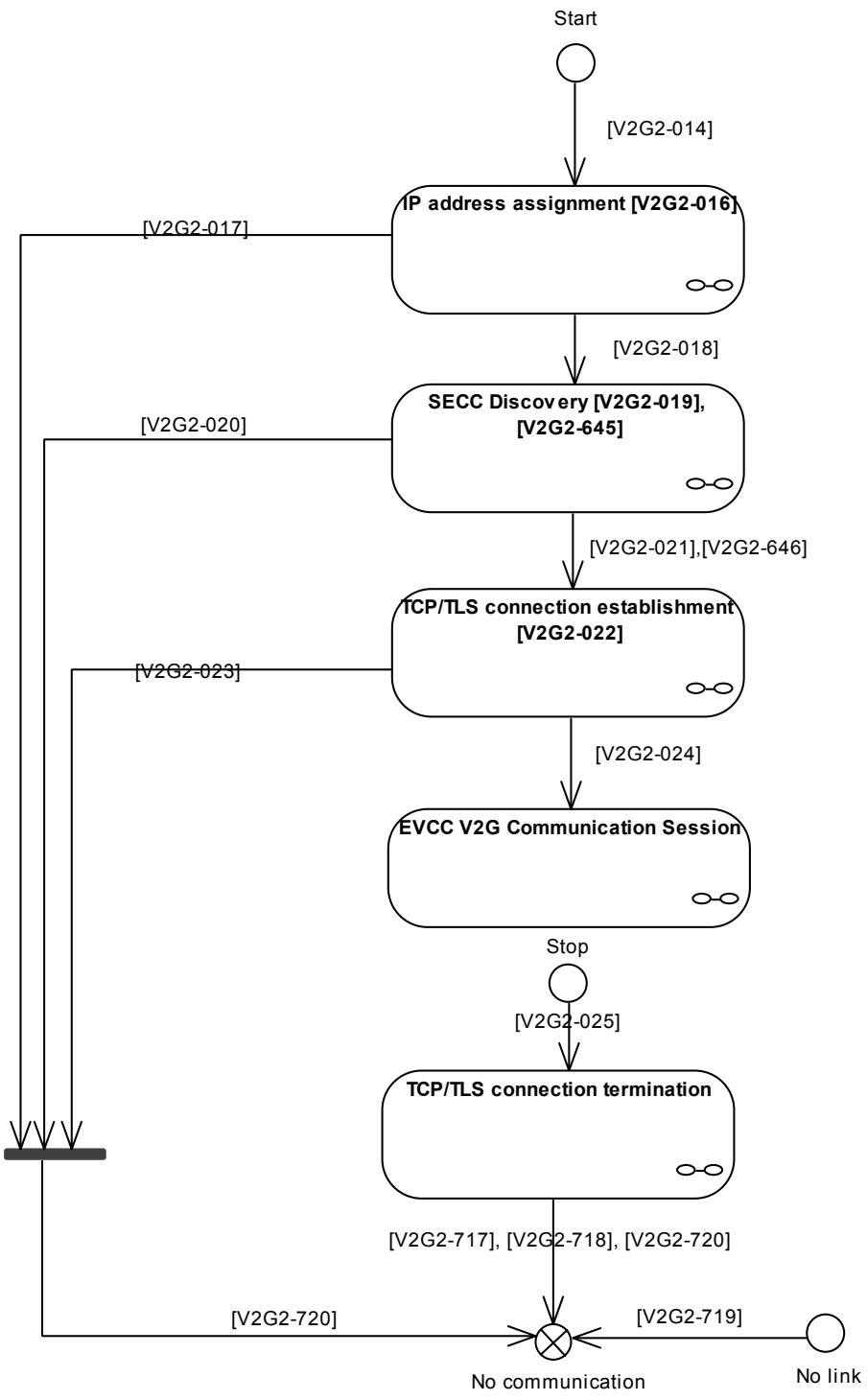


Figure 6 — Overview V2G communication states EVCC

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

The following applies for the SECC:

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

[V2G2-721] After indication of a successful Data-Link establishment (D-LINK_READY.indication(DLINKSTATUS=Link established), the SECC shall initiate the address assignment mechanism.

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

NOTE 1 To enable the integration of an SECC in different communication infrastructures, the definition of the address assignment for the SECC is out of scope of this standard. This enables the operator to assign an appropriate mechanism. E.g. the operator may chose any existing mechanism providing a valid IP address like e.g. a static IP or the mechanism described in subclauses 7.6.3.2 and 7.6.3.3.

NOTE 2 The SECC shall be configured with an valid IP address for enabling a connection to a EVCC. The IP assignment mechanism for the SECC has no impact on compatibility and is not defined by this standard.

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

NOTE 3 It is not required that the SECC discovery service is implemented in the SECC directly. It is also possible to have a separate unit providing the SECC discovery service.

[V2G2-723] The SECC shall stop the SDP server when SECC_CommunicationSetup_Timer is equal or larger than V2G_SECC _CommunicationSetup_Performance_Time.

[V2G2-029] The SECC shall stop the IP address assignment mechanism when V2G_SECC_CommunicationSetup_Timer is equal or larger than V2G_SECC_CommunicationSetup_Performance_Time.

[V2G2-030] After the SDP server is started successfully, the SECC shall wait for a TLS or TCP connection initialization depending on the SDP response message as defined in subclause 7.10.1.5..

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

[V2G2-032] The SECC shall stop waiting for establishing the TLS connection when V2G_SECC_CommunicationSetup_Timer is equal or larger than V2G_SECC_CommunicationSetup_Performance_Time.

[V2G2-033] After the TLS or TCP connection is established, the SECC shall wait for the initialization of the V2G Communication Session as defined in clause 8.

[V2G2-722] If **[V2G2-033]** applies the SECC can stop the SDP server after successful establishment of a TCP or TLS connection.

[V2G2-034] The SECC shall terminate the TLS or TCP connection after stopping the V2G Communication Session.

[V2G2-724] If the SECC received the message SessionStopReq with parameter ChargingSession equal to "Terminate" it shall terminate the Data-Link (D-LINK_TERMINATE.request()) after sending the message SessionStopRes.

[V2G2-725] If the SECC received the message SessionStopReq with parameter ChargingSession equal to "Pause" it shall pause the Data-Link (D-LINK_PAUSE.request()) after sending the message SessionStopRes and continue with **[V2G2-721]**.

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

[V2G2-727] If the SECC identifies any error it shall indicate an Data-Link error (D-LINK_ERROR.request()) and continue with **[V2G2-721]**.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

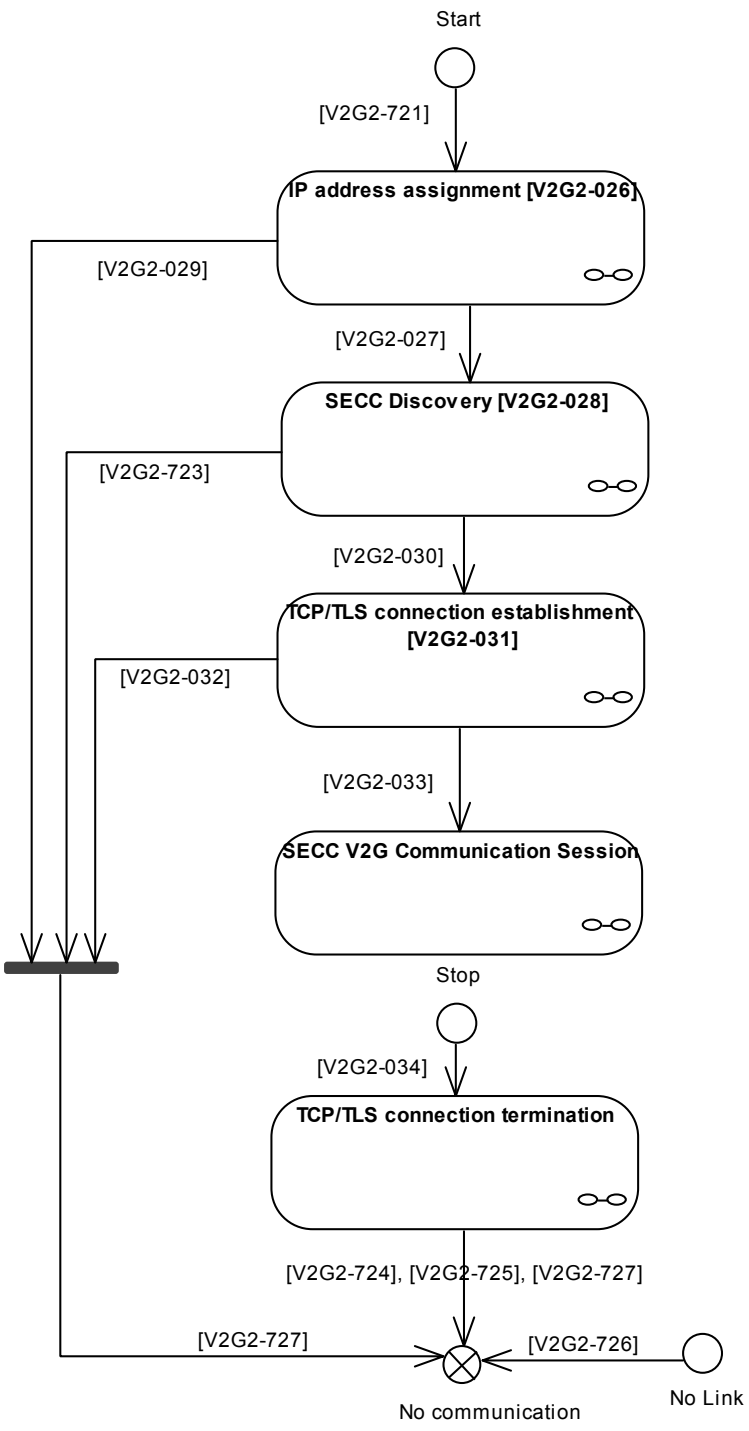


Figure 7 — Overview V2G Communication Session states SECC

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

7.5 Data Link Layer

The definitions in this document assume the Data Link layer to support the transport of IP packets as defined in the requirements. Part 3 of this standard defines additional details on Data Link Layer to be covered.

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

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

7.6 Network Layer

7.6.1 General

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

7.6.2 Applicable RFCs and limitations and protocol parameter settings

7.6.2.1 IPv6

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

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

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

NOTE 1 The IANA allocation guidelines for the routing type field in the IPv6 routing header are described in IETF RFC 5871. It is recommended to adhere to these guidelines.

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

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

NOTE 2 A V2G Entity should comply with the specification in IETF RFC 5220, which extends IETF RFC 2460.

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

NOTE 3 The communication between EVCC and secondary actors is out of scope of this Part of ISO 15118 and may or may not use IP fragmentation.

7.6.2.2 Dynamic Host Control Protocol (DHCPV6)

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

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

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

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

7.6.2.3 Neighbor Discovery (ND)

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

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

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

7.6.2.4 Internet Control Message Protocol (ICMP)

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

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

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

Table 5 — Mandatory ICMP Message Set

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

7.6.3 IP Addressing

7.6.3.1 General

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

— Link local IP address of EVCC

— Global IP address of EVCC, if router is present in local link

— IP address of SECC

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

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

7.6.3.2 Stateless auto address configuration (SLAAC)

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

[V2G2-051] The interface ID of the Link-Local address of a V2G Entity shall be generated from its IEEE 48 bit MAC identifier according to the definition in IETF RFC 4291.

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

[V2G2-053] If the SECC provides the Message Sets Certificate Install, Certificate Update, or Value Added Services as defined in subclause 8.6.2 it shall support IETF RFC 6106 for providing a DNS server address.

7.6.3.3 Address selection

[V2G2-054] If multiple IPv6 addresses are supported, the IPv6 Default Address Selection shall be performed according IETF RFC 3484.

7.7 Transport Layer

7.7.1 Transmission Control Protocol (TCP)

7.7.1.1 Overview

The Transmission Control Protocol (TCP) allows applications of V2G Entities to establish a reliable data connection to other entities. To exchange in a reliable way and in-order delivery of sender to receiver data. Additionally TCP provides flow control and congestion control and also provides for various algorithms to handle congestion and influence flow control.

7.7.1.2 Applicable RFCs, limitations and protocol parameter settings

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

7.7.1.3 TCP Performance and checksum requirements

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

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

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

[V2G2-058] Each V2G Entity should implement the NewReno Modification to TCP's Fast Recovery Algorithm according to IETF RFC 6582.

[V2G2-059] Each V2G Entity should compute TCP's retransmission timer according to IETF RFC 6298.

[V2G2-060] To increase TCP’s performance each V2G Entity should implement TCP Extensions for High Performance according to IETF RFC 1323.

[V2G2-061] Each V2G Entity should support TCP Selective Acknowledgment Options according to IETF RFC 2018.

[V2G2-062] Each V2G Entity should implement the User Timeout Option according to IETF RFC 5482.

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

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

It is recommended to use the following checksum algorithm:

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

7.7.2 User Datagram Protocol (UDP)

7.7.2.1 Overview

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

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

7.7.2.2 Applicable RFC, limitations and protocol parameter settings

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

7.7.3 Transport Layer Security (TLS)

7.7.3.1 Overview

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

7.7.3.2 Applicable RFCs

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

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

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

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

7.7.3.3 Transport Layer Security Usage

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

[V2G2-070] Each EVCC shall check the validity of the Sub-CA Certificates (in the SECCs certificate chain) via an OCSP response according to IETF RFC 6960, when TLS is used. The OCSP Requests

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

shall be transported as part of the TLS handshake using the extension defined in IETF RFC 6961.

NOTE 1 It is not intended, that the EVCC requests an OCSP response for an SECC leaf certificate during TLS handshake.

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

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

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

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

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

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

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

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

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

[V2G2-651] The EVCC shall send a list of V2G Root Certificates it possesses, an extension of type "trusted_ca_keys" in the (extended) client hello as defined in IETF RFC 6066.

[V2G2-871] If an SECC is deployed in an environment that is not a private environment, it shall send its own certificate and a chain up to a root (excluding the root certificate itself) which shall be one of those roots previously indicated by the EVCC as being present in the EVCC. If the EVCC has requested OCSP responses, for each certificate that the TLS server responds with, an OCSP response shall be sent to EVCC, as defined in IETF RFC 6961. The OCSP responder shall fill the field “certs” in the OCSP response (BasicOCSPResponse) structure according to IETF RFC 6960sec 4.2.1. The SECC shall also send the certificate of the OCSP responder if it is not the corresponding Sub-CA itself.

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

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

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

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

NOTE 7 This supports the “pairing mode”

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

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

— If the TLS server certificate chain contains only one leaf certificate and one root certificate, which is one of the root certificates that the EV has stored as a private root, the EV ignores the fact, that the server has not sent OCSP responses.

— If the TLS server certificate chain is linked to a V2G root, the EVCC shall abort the TLS connection.

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

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

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

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

7.7.3.4 Transport Layer Security Credentials and Cipher Suites

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

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

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

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

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

Table 6 — TLS authentication

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

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

[V2G2-603] The EVCC shall support at least one cipher suite as listed in Table 7, if TLS is used.

Additional cipher suites may be supported by any V2G Entity.

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

Table 7 — Supported cipher suites

Cipher suite	RFC
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	IETF RFC 5289
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	IETF RFC 5289

7.8 V2G Transfer Protocol

7.8.1 General Information

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

7.8.2 Supported ports

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

Table 8 — Supported TCP ports for V2GTP

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

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

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

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

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

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

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

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

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

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

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

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

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

7.8.3 Protocol Data Unit

7.8.3.1 Structure

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

Header (8 Bytes)	Payload (0-4294967295 Bytes)

Figure 8 — V2GTP Message structure

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

The V2GTP message header structure is shown in Figure 9 and described in Table 9. The supported payload types are described in Table 10.

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

Figure 9 — V2GTP Message header structure

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

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

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

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

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

Table 9 — Generic V2GTP header structure

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

Table 10 — Overview on V2GTP payload types

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

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

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

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

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

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

7.8.3.2 Header Processing

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

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

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

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

[V2G2-094] A V2GTP entity shall check the Payload Length after the successful check of the Payload Type.

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

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

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

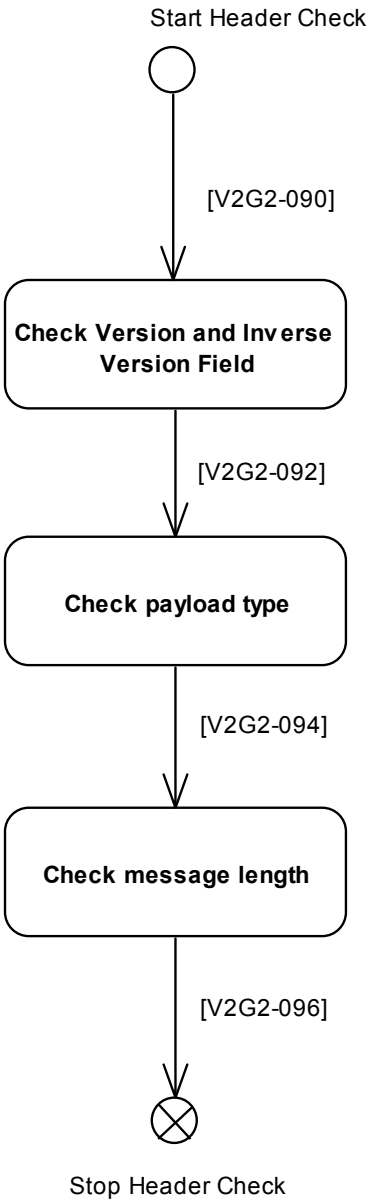


Figure 10 — V2GTP generic header handler

7.9 Presentation Layer

7.9.1 XML and Efficient XML Interchange (EXI)

7.9.1.1 Overview

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

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

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

7.9.1.2 Efficient XML Interchange

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

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

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

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

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

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

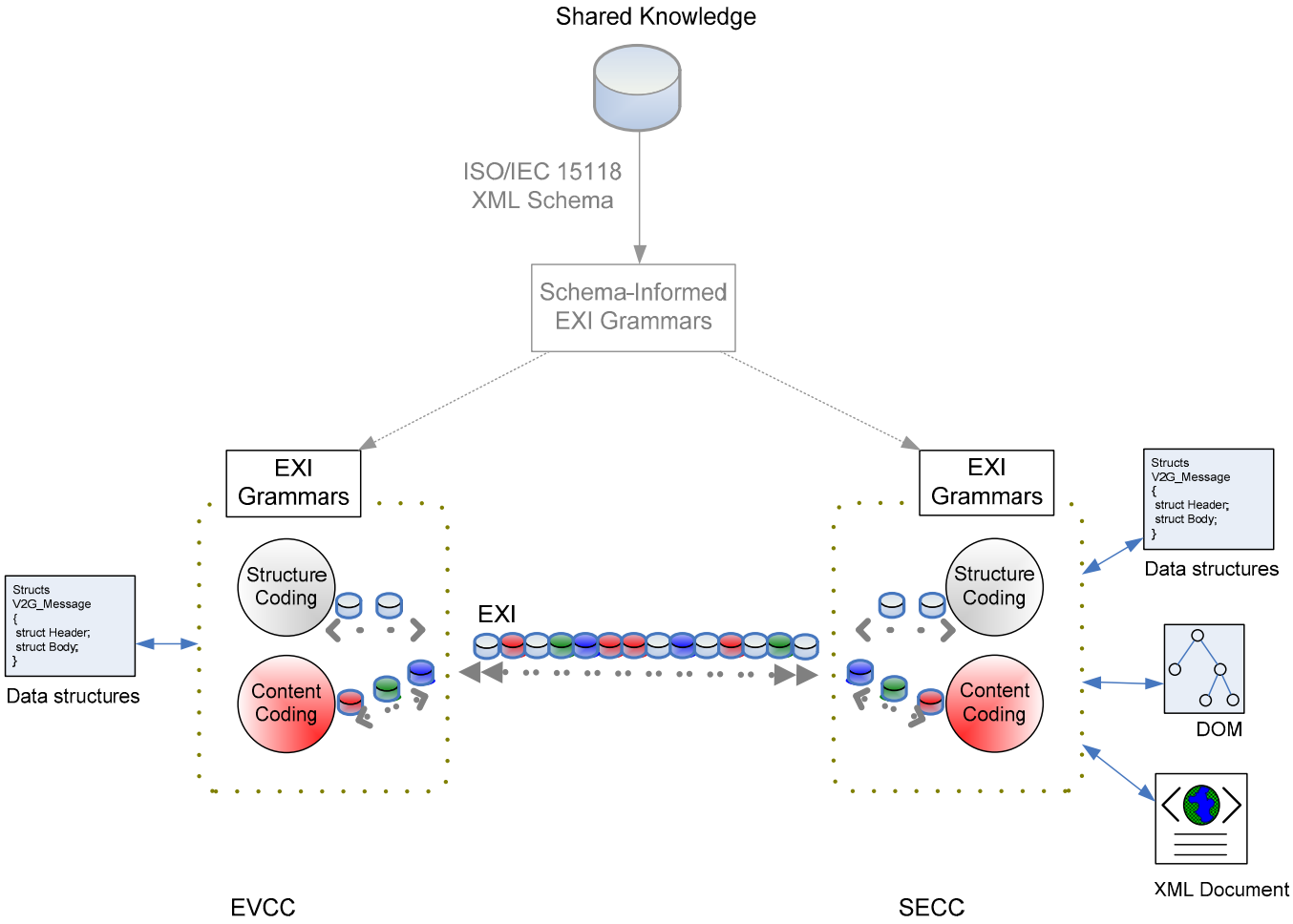


Figure 11 — Basic concept of EXI applied to V2G communication

7.9.1.3 EXI Settings for application layer messages

The following EXI settings are used for the EXI-based V2G communication.

[V2G2-098] The XML Schema with the namespace “urn:iso:15118:2:2013:MsgDef” that represents this ISO 15118 version 2.0 (major version “2”, minor version “0”) shall be used for encoding and decoding EXI streams.

[V2G2-099] The EXI coder for encoding and decoding of the ISO 15118 communication shall use the default EXI coding options according to W3C EXI 1.0 subclause "EXI Options" with the exception of the options listed in Table 11.

Table 11 — EXI option settings

EXI Option	Description	ISO 15118 value
valuePartitionCapacity	Specifies the total capacity of value partitions in a string table	0

[V2G2-100] The EXI header (refer to W3C EXI 1.0 clause "Header") shall be used in a way that fulfils the ISO 15118 needs. That means, the optional EXI Cookie ($EXI) shall never be used and the Presence Bit for EXI Options shall be always set to 0 (=false). As a consequence the optional EXI Options shall never be part of an ISO 15118 message. Each EXI implementation (on EVCC or SECC side) shall discard messages that do not respect the ISO 15118 EXI header options.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

[V2G2-101] An element/attribute which is not defined in “urn:iso:15118:2:2013:MsgDef” namespace shall be encoded and decoded as schema deviation case according to W3C EXI 1.0 subclause "Adding Productions when Strict is False".

[V2G2-600] The EXI coder for encoding and decoding of the ISO 15118 communication shall use the EXI profile settings W3C EXI Profileaccording to Table 12.

NOTE For details describing the EXI profile refer to W3C EXI Profile.

Table 12 — EXI profile settings

EXI profile parameter	Description	ISO 15118 value
maximumNumberOfBuiltInElementGrammars	This option is the maximum number of built-in element grammars for which dynamically productions other than AT(xsi:type) productions have been added.	0
maximumNumberOfBuiltInProductions	This option is the maximum number of top-level productions that can be dynamically inserted in built-in element grammars excluding AT(xsi:type) productions.	0

[V2G2-102] A simple type/value of an element/attribute which is not defined in the “urn:iso:15118:2:2013:MsgDef” namespace shall be encoded and decoded type-aware.

7.9.2 Message Security

7.9.2.1 Overview

XML Signature is a W3C recommendation that addresses the authenticity requirements of some data fragments (e.g. metering information) of the XML-based V2G. XML Signature defines a mechanism by which messages and message parts can be digitally signed to provide integrity, to ensure that the data is not tampered with, and authentication, to verify the identity of the message producer. For protecting confidentiality, a hybrid encryption scheme based on the Diffie-Hellman-Protocol is applied.

7.9.2.2 Application layer credentials and cipher suites

Credentials to be applied on application layer shall be suitable for the targeted XML security. Here, XML signature is chosen to protect billing relevant information between EVCC, SECC and/or SA. Moreover, binary encryption provides a confidentiality protected way for private key provisioning to the EVCC without having intermediaries access this private key. Both approaches require asymmetric key material. The credentials for EVCC signing are provided by the Contract Certificate and credentials for EVCC receiving encrypted data are provided by an ECDH key exchange as described in Annex G.

[V2G2-103] The maximum lifetime of the ContractCertificate shall be no longer than 2 years.

[V2G2-104] The minimum lifetime of the certificate used for XML signature and providing mechanisms for encryption shall be 4 weeks. If the contract lifetime is less, the certificate validity period shall be mapped to the contract lifetime.

NOTE 1 For explanation of certificate validity period refer to Annex E.1

NOTE 2 If the certificate is not used for charging it might be used for provisioning. An OEM Provisioning Certificate enables an EVCC to request a valid Contract Certificate for plug and charge.

NOTE 3 The private keys of the Contract Certificate and the OEM Provisioning Certificate are sensitive data. Once a private key gets compromised, it cannot be trusted anymore and therefore should not be used anymore. If one of these private keys could be read by an attacker, the attacker could impersonate the original EVCC and receive electricity at the expense of the original vehicle owner. As a countermeasure, the EVCC may choose to additionally protect said keys. This may range from simple security measures such as setting readout protection fuse bits in the EVCC microcontroller to more advanced protection via secure boot facilities, debug access protection, and embedded hardware security modules (HSM). The latter offer a high level of security including protection against physical attacks. A suitable HSM provides a

AVA Documents
Document Sharing Hub

© ISO 2014 – All rights reserved

Full document details: BS EN ISO 15118-2:2016

secure environment for private key operations. It offers interfaces to use the private key but ensures that the key 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 may be integrated into the EVCC as a separate physical package or as an on-chip microcontroller extension.

NOTE 4 In order to reduce the number of required certificate update requests for the EV, the mobility operator which issues the charging contract certificates, is suggested to choose longer validity periods (up to maximum), if this is meaningful with regards to contract validity period and cancellation period.

7.9.2.3 Contract Certificates as XML signature credentials

Contract Certificate is bound to a EMAID and used in XML signature to authorize the vehicle for charging. The Contract Certificate can be verified even if the SECC is offline. The contract binding is handled as follows:

[V2G2-108] The EMAID shall be encoded in the subject of the certificate.

7.9.2.4 XML Security specifics for 'PnC' Message Set(s)

7.9.2.4.1 XML Data Structures for Application Layer Security

Security on Application Layer is provided using signature and encryption of messages. Information targeted for SA services is exchanged using XML data structures. Consequently, this information can be protected end-to-end using XML Security.

Typical information exchanged between EVCC and SECC:

Signed meter reading approval from the vehicle used for online and semi-online connections. The meter readings from the SECC are sent via the TLS protected tunnel. They may include the signature of the electricity meter providing source authentication to protect them additionally. The vehicle in turn signs the meter readings to provide a base for the billing process if local regulations permit it. This approach saves the meter reading signatures on the SECC side. The meter readings are cumulated so that the latest signed meter reading is the base for the billing. Here XML Signatures are used. They ensure integrity protection with the possibility for all intermediate and participating entities to rely on this information.

7.9.2.4.2 XML Signature mechanism

This subclause is intended as an introduction to XML Signatures.

NOTE 1 For an Overview on XML Signatures see also Annex J.

XML Signatures as defined in W3C XML Signature Syntax and Processing Version 1.1 can be applied to arbitrary digital content (data objects) in the same way as digital signatures are calculated. When applying a digital signature to data objects, the data objects are first digested (hashed) and the result is then signed using an asymmetric algorithm like RSA or ECDSA. In the case of XML, the digest is placed in an XML element, together with additional information. This element is then hashed and cryptographically signed. This standard uses detached XML Signatures according to W3C XML Signature Syntax and Processing Version 1.1. That means the signature and data can be in separate (externally detached) or in the same XML document (internally detached) as sibling elements. The signature may comprise only a part of the XML document referenced by an ObjectID.

Figure 12 shows the schema diagram of the XML Signature element included in the V2G message header.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

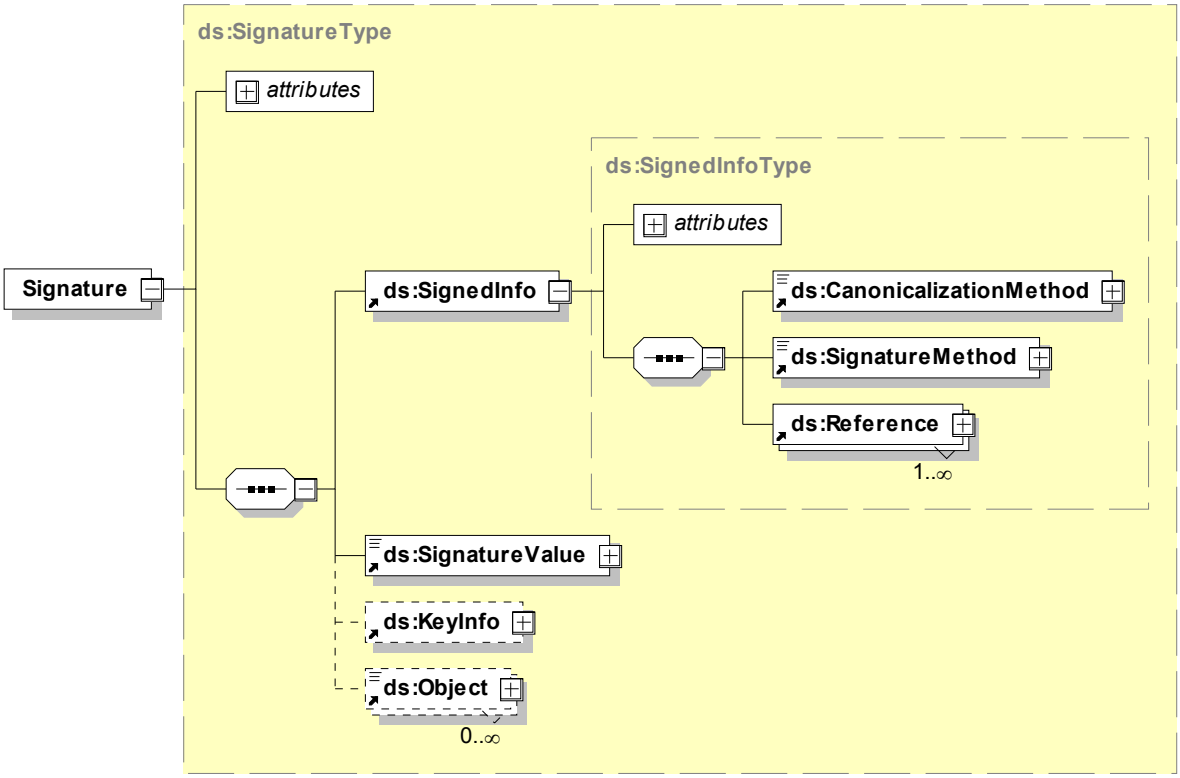


Figure 12 — Schema Diagram – XML Signature

Figure 13 shows the schema diagram of the element Reference included in the element SignedInfo which is part of the XML Signature depicted in Figure 12.

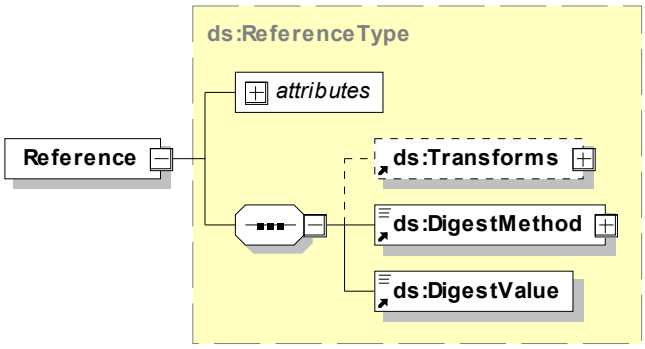


Figure 13 — Schema Diagram – Element Reference included in element SignedInfo

NOTE 2 The meter values from the SECC may already been signed. This signature value is treated as informational element and is required for the gauging process. It may optionally be checked by the vehicle. The signature may comprise also the meter ID.

[V2G2-117] Each V2G Entity shall support detached XML signatures.

[V2G2-119] For XML signature operations, the data which gets signed, shall be the EXI representation of this data.

[V2G2-764] As canonicalization method EXI with schema-informed fragment grammar shall be used.

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016

[V2G2-765] Each message, that needs the XML Signature framework shall use the value "http://www.w3.org/TR/canonical-exi/" as Algorithm attribute within the CanonicalizationMethod element.

[V2G2-766] Each message, that needs the XML Signature framework shall use the value "http://www.w3.org/TR/canonical-exi/".as Algorithm attribute within the Transform element.

[V2G2-767] The maximum number of Transforms is limited to one (1) (i.e. per referenced element where a signature is to be transmitted for, just one single Transform algorithm can be indicated).

[V2G2-768] "The parts which have to be signed in the XML-based messages shall be encoded as EXI schema-informed fragment.

[V2G2-769] Each message, that needs the XML Signature framework shall use the value "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256" as Algorithm attribute within the SignatureMethod element.

[V2G2-770] Each message, that needs the XML Signature framework shall use the value " http://www.w3.org/2001/04/xmlenc#sha256" as Algorithm attribute within the DigestMethod element.

[V2G2-771] The following message elements of the XML Signature framework shall not be used when transmitting signatures in the header of the a V2G message:

- Id (attribute in SignedInfo)
- ##any in SignedInfo – CanonicalizationMethod
- HMACOutputLength in SignedInfo – SignatureMethod
- ##other in SignedInfo – SignatureMethod
- Type (attribute in SignedInfo-Reference)
- ##other in SignedInfo – Reference – Transforms – Transform
- XPath in SignedInfo – Reference – Transforms – Transform
- ##other in SignedInfo – Reference – DigestMethod
- Id (attribute in SignatureValue)
- Object (in Signature)
- KeyInfo

[V2G2-909] The signature shall not reference more than 4 signed elements.

NOTE 3 This allows to determine an upper bound for the size of the signature header.

For the application of XMLDsig, any element which should be signed must be addressable. In this standard, this is achieved by an URI referencing the ID attribute of such an element. Therefore, any message element that is signed carries an ID attribute. If a specific element is to be signed in all use cases, the ID attribute is marked mandatory in the XSD. Otherwise, if it is signed in only some use cases, the ID attribute is marked optional and can be omitted when not needed.

NOTE 4 Presence of an ID attribute does not necessarily indicate that a signature is used, i.e. if no signature is used, an ID can be present nevertheless.

7.9.2.4.3 Encryption mechanism

Private keys belonging to contract certificates need to be protected (i.e. encrypted) when distributed from the SA to the EVCC. For a more detailed explanation please refer to Annex G.

[V2G2-121] The EVCC shall support calculation of the ECDH secret and the key derivation function for the decryption of encrypted information like private keys.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 15118-2:2016