

DIN EN ISO 15118-2:2022-11 (E)

Erscheinungsdatum: 2022-10-21

Road vehicles - Vehicle-to-Grid Communication Interface - Part 2: Network and application protocol requirements (ISO/DIS 15118-2:2022); English version prEN ISO 15118-2:2022, only on CD-ROM

Contents	Page
Foreword.....	vii
Introduction.....	viii
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions.....	3
4 Symbols and abbreviated terms.....	6
5 Conventions.....	7
5.1 Definition of OSI based services.....	7
5.2 Requirement structure.....	8
5.3 Usage of RFC references.....	8
5.4 Notation used for XML schema diagrams.....	8
6 Document overview.....	8
7 Basic requirements for V2G communication.....	9
7.1 General information.....	9
7.2 Service primitive concept of OSI layered architecture.....	10
7.2.1 Overview.....	10
7.2.2 Syntax of service primitives.....	10
7.3 Security concept.....	11
7.3.1 Call flows (flow charts).....	11
7.3.2 Certificate and key management.....	15
7.3.3 Number of root certificates and root validity, certificate depth and size.....	17
7.3.4 Support and application of TLS.....	18
7.4 V2G communication states and data link handling.....	20
7.5 Data link layer.....	25
7.6 Network layer.....	25
7.6.1 General.....	25
7.6.2 Applicable RFCs and limitations and protocol parameter settings.....	25
7.6.3 IP addressing.....	26
7.7 Transport layer.....	27
7.7.1 Transmission control protocol (TCP).....	27
7.7.2 User datagram protocol (UDP).....	28
7.7.3 Transport layer security (TLS).....	28
7.8 V2G transfer protocol.....	31
7.8.1 General.....	31
7.8.2 Supported ports.....	31
7.8.3 Protocol data unit.....	33
7.9 Presentation layer.....	36
7.9.1 XML and efficient XML interchange (EXI).....	36
7.9.2 Message security.....	39
7.10 Application layer.....	46
7.10.1 SECC discovery protocol.....	46
7.10.2 Vehicle to grid application layer messages.....	51
7.10.3 Application layer service primitives.....	51
8 Application layer messages.....	55
8.1 General.....	55
8.2 Protocol handshake definition.....	56
8.2.1 Handshake sequence.....	56

8.2.2	Message definition supportedAppProtocolReq and supportedAppProtocolRes	57
8.2.3	Semantics description supportedAppProtocol messages	57
8.2.4	Message examples.....	58
8.3	V2G message definition.....	60
8.3.1	General.....	60
8.3.2	Message definition.....	60
8.3.3	Message header definition.....	61
8.3.4	Message body definition	62
8.4	V2G communication session and BodyElement definitions	63
8.4.1	General.....	63
8.4.2	Session handling.....	63
8.4.3	Common messages.....	66
8.4.4	AC messages	96
8.4.5	DC messages.....	98
8.5	Complex data types.....	107
8.5.1	Overview	107
8.5.2	Common.....	107
8.5.3	AC	132
8.5.4	DC.....	136
8.6	Identification modes and message set definitions	142
8.6.1	Overview	142
8.6.2	Supported message sets.....	145
8.6.3	Selection of message sets	172
8.7	V2G communication timing	177
8.7.1	Overview	177
8.7.2	Message sequence and communication session	178
8.7.3	Session setup and ready to charge.....	183
8.7.4	V2G message synchronization with IEC 61851-1 signalling.....	186
8.8	Message sequencing and error handling.....	191
8.8.1	Overview	191
8.8.2	Basic Definitions for Error Handling.....	192
8.8.3	ResponseCode handling.....	192
8.8.4	Request-response message sequence requirements.....	196
8.9	Request-response message sequence examples.....	215
8.9.1	AC	215
8.9.2	DC.....	218
Annex A (normative) Schema definition.....		223
A.1	Overview.....	223
A.2	V2G_CI_AppProtocol.xsd	224
A.3	V2G_CI_MsgDef.xsd.....	224
A.4	V2G_CI_MsgHeader.xsd.....	225
A.5	V2G_CI_MsgBody.xsd	225
A.6	V2G_CI_MsgDataTypes.xsd	232
A.7	xmldsig-core-schema.xsd	242
Annex B (normative) Certificate profiles.....		247
B.1	Overview.....	247
Annex C (normative) Specification of identifiers.....		253
C.1	e-Mobility account identifier (EMAID)	253

C.1.1	EMAID syntax	253
C.1.2	EMAID Semantics	253
C.1.3	Calculation of the check digit	254
C.2	Electric vehicle supply equipment ID (EVSEID).....	254
C.2.1	EVSEID syntax	254
C.2.2	EVSEID semantics	254
Annex D (informative)	Mapping of ISO 15118-1 use case elements	256
D.1	Relation of identification modes and use case elements.....	256
Annex E (informative)	Mapping of ISO 15118 message element names to SAE J2847/2 terms	309
E.1	SAE J2847/2 status codes.....	309
E.2	SAE J2847/2 energy transfer types	310
E.3	SAE J2847/2 signals	311
Annex F (informative)	Message examples	313
F.1	Value added service selection	313
F.2	EXI encoded message examples.....	315
F.2.1	SessionSetupRes message	315
F.2.2	ChargeParameterDiscoveryReq message (AC-based).....	315
F.2.3	CurrentDemandReq message.....	316
F.3	Schedules and tariff information	317
F.3.1	Overview.....	317
F.3.2	Dynamic GridSchedule w/o SalesTariff over ISO 15118 V2G CI.....	317
F.3.3	“Time Of Use”-based SalesTariff with constant value for GridSchedule.....	319
F.3.4	“Time Of Use”-based SalesTariff with dynamic GridSchedule.....	320
F.3.5	“Consumption”-based SalesTariff with constant value for GridSchedule	322
F.3.6	Multiple SalesTariffs with different demand Limits in GridSchedule	323
F.3.7	Time of Use-based SalesTariffs including relativePricePercentage	325
Annex G (informative)	Application of certificates	333
G.1	General information	333
G.1.1	Overview.....	333
G.1.2	Demands of the OEM.....	334
G.1.3	Demands of the secondary actors.....	334
G.1.4	Rationale for decisions in this document	335
G.1.5	Overview of the resulting certificate structure	337
G.2	Simplified certificate management in private environment.....	338
G.2.1	Overview (motivation)	338
G.2.2	Solution for private environments.....	338

G.2.2.1 General	338
G.2.2.2 Installation of a private root certificate into a vehicle	339
G.2.2.3 Charging in a private environment	339
G.2.2.4 Compromised certificate of a wall box	339
G.3 Use of OEM provisioning certificates	340
G.3.1 Introduction	340
G.3.2 Processes	341
G.3.2.1 Vehicle production	341
G.3.2.2 Vehicle Hand-Over	341
G.3.2.3 Contract Conclusion	342
G.3.2.4 Certificate installation	342
G.3.2.5 Certificate update	342
G.3.2.6 Component replacement	342
G.4 Security appliances and their associated certificates	343
Annex H (informative) Encryption for the distribution of secret keys	346
H.1 Overview	346
H.2 Ephemeral-static Diffie-Hellman key agreement	346
H.3 Key pairs	347
Annex I (informative) Message sequencing for renegotiation	348
I.1 Overview	348
I.2 Renegotiation after resuming a V2G communication session	351
Annex J (informative) Overview on XML signatures	352
J.1 Overview	352
J.2 Signature generation	352
J.3 Signature generation for secondary actors	355
J.4 Signature validation	355
Annex K (informative) Summary of requirements	356
Bibliography	362