



SLOVENSKI STANDARD
oSIST prEN IEC 63380-3:2024
01-julij-2024

Sistemi za upravljanje lokalnih polnilnih postaj in lokalni sistemi za upravljanje z energijo za povezovanje v omrežje in izmenjavo informacij - 3. del: Posebni vidiki komunikacijskih protokolov in kibernetске varnosti

Local charging station management systems and local energy management systems network connectivity and information exchange - Part 3: Communication protocol and cybersecurity specific aspects

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

Ta slovenski standard je istoveten z: prEN IEC 63380-3:2024

[oSIST prEN IEC 63380-3:2024](https://standards.iteh.ai/catalog/standards/sist/e17457d1-9588-4a9d-937f-4175e5552398/osist-pr-en-iec-63380-3-2024)

<https://standards.iteh.ai/catalog/standards/sist/e17457d1-9588-4a9d-937f-4175e5552398/osist-pr-en-iec-63380-3-2024>

ICS:

29.240.99	Druga oprema v zvezi z omrežji za prenos in distribucijo električne energije	Other equipment related to power transmission and distribution networks
43.120	Električna cestna vozila	Electric road vehicles

oSIST prEN IEC 63380-3:2024

en



COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER:

IEC 63380-3 ED1

DATE OF CIRCULATION:

2024-05-10

CLOSING DATE FOR VOTING:

2024-08-02

SUPERSEDES DOCUMENTS:

69/878/CD, 69/950/CC

IEC TC 69 : ELECTRICAL POWER/ENERGY TRANSFER SYSTEMS FOR ELECTRICALLY PROPELLED ROAD VEHICLES AND INDUSTRIAL TRUCKS	
SECRETARIAT: Belgium	SECRETARY: Mr Peter Van den Bossche
OF INTEREST TO THE FOLLOWING COMMITTEES:	PROPOSED HORIZONTAL STANDARD: <input checked="" type="checkbox"/> Other TC/SCs are requested to indicate their interest, if any, in this CDV to the secretary.
FUNCTIONS CONCERNED: <input type="checkbox"/> EMC <input type="checkbox"/> ENVIRONMENT <input type="checkbox"/> QUALITY ASSURANCE <input type="checkbox"/> SAFETY	
<input checked="" type="checkbox"/> SUBMITTED FOR CENELEC PARALLEL VOTING Attention IEC-CENELEC parallel voting The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting. The CENELEC members are invited to vote through the CENELEC online voting system.	<input type="checkbox"/> NOT SUBMITTED FOR CENELEC PARALLEL VOTING

oSIST prEN IEC 63380-3:2024

<http://standards.iteh.ai/catalog/standards/sist/63380-3-2024/osist-pr-en-iec-63380-3-2024>

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any relevant "In Some Countries" clauses to be included should this proposal proceed. Recipients are reminded that the CDV stage is the final stage for submitting ISC clauses. (SEE [AC/22/2007](#) OR [NEW GUIDANCE DOC](#)).

TITLE:

<p>Local Charging station management systems and Local Energy Management Systems network connectivity and information exchange - Part 3 Communication Protocol and Cybersecurity Specific Aspects</p>

PROPOSED STABILITY DATE: 2027

NOTE FROM TC/SC OFFICERS:

Copyright © 2024 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

2	CONTENTS	
3		
4	FOREWORD.....	7
5	INTRODUCTION.....	9
6	1 Scope.....	10
7	2 Normative references	10
8	3 Terms, definitions, and abbreviated terms	11
9	3.1 Terms and definitions.....	11
10	3.2 Abbreviated terms.....	15
11	4 Reader's Guide	15
12	4.1 General.....	15
13	5 SPINE Protocol	16
14	5.1 General.....	16
15	5.2 Architecture overview.....	16
16	5.2.1 General rules.....	16
17	5.2.2 Common data types.....	17
18	5.2.3 Address level details.....	21
19	5.3 SPINE Datagram	23
20	5.3.1 Introduction	23
21	5.3.2 Header	24
22	5.3.3 Payload	31
23	5.4 Communication modes.....	44
24	5.4.1 Simple communication mode	45
25	5.4.2 Enhanced communication mode	45
26	5.5 Functional commissioning.....	46
27	5.5.1 Detailed discovery	46
28	5.5.2 Destination list.....	60
29	5.5.3 Binding	64
30	5.5.4 Subscription	73
31	5.5.5 Use Case discovery.....	81
32	6 SHIP.....	84
33	6.1 Architecture overview.....	84
34	6.1.1 General	84
35	6.1.2 General considerations on Closing communication channels	85
36	6.1.3 SHIP node parameters	85
37	6.2 Registration	87
38	6.2.2 Successful registration	88
39	6.2.3 Registration details and recommendations (informative).....	88
40	6.3 Reconnection.....	89
41	6.3.1 General	89
42	6.3.2 Reconnection details in case of changed key material (informative).....	90
43	6.4 Discovery.....	90
44	6.4.1 General	90
45	6.4.2 Service instance	90
46	6.4.3 Service name	91
47	6.4.4 Multicast DNS name	91

48	6.4.5	Recommendations for re-discovery	93
49	6.5	TCP	93
50	6.5.1	General	93
51	6.5.2	Limited connection capabilities	94
52	6.5.3	Online detection	94
53	6.5.4	TCP connection establishment.....	94
54	6.5.5	Retransmission timeout	95
55	6.6	TLS.....	95
56	6.6.1	General	95
57	6.6.2	Cipher suites	96
58	6.6.3	Maximum fragment length.....	96
59	6.6.4	TLS compression.....	97
60	6.6.5	Renegotiation	97
61	6.6.6	Session resumption	97
62	6.6.7	TLS extension for ECC	98
63	6.6.8	TLS probing.....	98
64	6.7	WebSocket	99
65	6.7.1	General	99
66	6.7.2	TLS dependencies	99
67	6.7.3	Opening handshake.....	99
68	6.7.4	Data framing.....	99
69	6.7.5	Connection keepalive	100
70	6.8	Message representation using JSON text format.....	100
71	6.8.1	Introduction	100
72	6.8.2	Definitions	101
73	6.8.3	Examples for each type	101
74	6.8.4	XML to JSON transformation	101
75	6.8.5	JSON to XML transformation	107
76	6.9	Key management.....	108
77	6.9.1	General	108
78	6.9.2	Certificates	109
79	6.9.3	SHIP node specific public key.....	113
80	6.9.4	Verification procedure.....	115
81	6.9.5	Symmetric key	122
82	6.9.6	SHIP node PIN	122
83	6.9.7	SHIP commissioning tool	123
84	6.9.8	QR Code	125
85	6.10	SHIP data exchange	129
86	6.10.1	Introduction	129
87	6.10.2	Terms in the context of SHIP Data Exchange	129
88	6.10.3	Protocol architecture / hierarchy	131
89	6.10.4	SHIP message exchange.....	132
90	6.11	Well-known protocolId.....	178
91	7	ECHONET Lite	178
92	7.1	General.....	178
93	Annex A (normative)	SHIP XSD	180
94	Bibliography	186
95			

96	Figure 1 – Overview of communication protocols within IEC 63380-3.....	16
97	Figure 2 – PossibleOperationsType	20
98	Figure 3 – DeviceAddressType	20
99	Figure 4 – EntityAddressType	21
100	Figure 5 – FeatureAddressType	21
101	Figure 6 – SPINE datagram	23
102	Figure 7 – SPINE header	24
103	Figure 8 – SPINE payload.....	32
104	Figure 9 – Example of selectors part (extract) with entity address part.....	43
105	Figure 10 – Communication modes of SPINE devices A, B and C.	44
106	Figure 11 – Discovery example.....	47
107	Figure 12 – Hierarchy types	47
108	Figure 13 – Function Discovery Example over Feature Description	48
109	Figure 14 – nodeManagementDetailedDiscoveryData function overview, part 1	52
110	Figure 15 – nodeManagementDetailedDiscoveryData function overview, part 2:	
111	deviceInformation.description	52
112	Figure 16 – nodeManagementDetailedDiscoveryData function overview, part 3:	
113	entityInformation.description	53
114	Figure 17 – nodeManagementDetailedDiscoveryData function overview, part 4:	
115	featureInformation.description.....	53
116	Figure 18 – nodeManagementDestinationListData function overview, part 1	62
117	Figure 19 – nodeManagementDestinationListData function overview, part 2	63
118	Figure 20 – Binding request	65
119	Figure 21 – nodeManagementBindingRequestCall function overview	66
120	Figure 22 – nodeManagementBindingData function overview.....	67
121	Figure 23 – nodeManagementBindingDeleteCall function overview	70
122	Figure 24 – Subscription request	74
123	Figure 25 – nodeManagementSubscriptionRequestCall function overview.....	75
124	Figure 26 – nodeManagementSubscriptionData function overview	76
125	Figure 27 – nodeManagementSubscriptionDeleteCall function overview	79
126	Figure 28 – nodeManagementUseCaseData function	82
127	Figure 29 – Physical Connections in the Overall System.....	84
128	Figure 30 – SHIP Stack Overview	85
129	Figure 31 – Full TLS 1.2 Handshake with mutual authentication.....	96
130	Figure 32 – Quick TLS Handshake with Session Resumption.....	97
131	Figure 33 – Easy Mutual Authentication with QR-codes and Smart Phone	122
132	Figure 34 – QR Code Model 2, "low" error correction code level, 0.33mm/Module, with	
133	SKI and PIN.....	128
134	Figure 35 – QR Code Model 2, "low" error correction code level, 0.33mm/module, with	
135	all values	128
136	Figure 36 – QR Code Model 2, "low" error correction code level, 0.33mm/module, with	
137	brainpoolP256r1 SKI and brainpoolP384r1 SKI	128
138	Figure 37 – Protocol Architecture and Hierarchy	131
139	Figure 38 – CMI Message Sequence Example	136

140	Figure 39 – Connection State "Hello" Sequence Example Without Prolongation	
141	Request: "A" and "B" already trust each other; "B" is slower/delayed.	144
142	Figure 40 – Connection State "Hello" Sequence Example With Prolongation Request.	145
143	Figure 41 – Connection State "Protocol Handshake" Message Sequence Example.	151
144	Figure 42 – Connection State "PIN verification" Message Sequence Example (Begin)	161
145	Figure 43: ECHONET Lite frame format.	179
146		
147	Table 1 – Structure of the SPINE datagram.	23
148	Table 2 – cmdClassifier values and kind of messages for a message "M" and the scope	
149	of related acknowledgement messages.	27
150	Table 3 – Structure of the SPINE header.	30
151	Table 4 – Elements of the SPINE payload.	32
152	Table 5 – Example table (template): This template is used in the subsequent sections	
153	for specific cmdOptions combinations. In this template, each "..." is just a placeholder.	35
154	Table 6 – Considered cmdOptions combinations for classifier "write".	36
155	Table 7 – Considered cmdOptions combinations for classifier "notify".	38
156	Table 8 – Considered cmdOptions combinations for classifier "read".	39
157	Table 9 – Considered cmdOptions combinations for classifier "reply".	39
158	Table 10 – Address path examples.	43
159	Table 11 – Notify/response list of entities and their corresponding features with	
160	nodeManagementDetailedDiscoveryData.	54
161	Table 12 – nodeManagementDetailedDiscoveryDataSelectors.	59
162	Table 13 – Notify/response of DestinationList information with	
163	nodeManagementDestinationListData.	63
164	Table 14 – Binding request with nodeManagementBindingRequestCall.	66
165	Table 15 – nodeManagementBindingData holds list of binding entries.	68
166	Table 16 – Remove Binding with nodeManagementBindingDeleteCall.	71
167	Table 17 – Subscription request with nodeManagementSubscriptionRequestCall.	75
168	Table 18 – nodeManagementSubscriptionData holds list of subscription entries.	77
169	Table 19 – Remove subscription with nodeManagementSubscriptionDeleteCall.	80
170	Table 20 – nodeManagementUseCaseData.	82
171	Table 21 – SHIP Parameters Default Values.	86
172	Table 22 – Mandatory Parameters in the TXT Record.	91
173	Table 23 – Optional Parameters in the TXT Record.	92
174	Table 24 – Mapping from the XSD Types to JSON Types.	102
175	Table 25 – Transformation of a simple type.	102
176	Table 26 – Mapping from the XSD compositors to JSON Types.	103
177	Table 27 – Examples for XML and JSON representations.	104
178	Table 28 – Example transformation of several combined XSD item types.	106
179	Table 29 – Example for JSON to XML transformation.	108
180	Table 30 – Trust Levels.	121
181	Table 31 – MessageType Values.	133
182	Table 32 – Structure of SmeHelloValue of SME "hello" Message.	137
183	Table 33 – Structure of SmeProtocolHandshakeValue of SME "Protocol Handshake"	
184	Message.	146

185	Table 34 – Structure of SmeProtocolHandshakeErrorValue of SME "Protocol	
186	Handshake Error" Message	147
187	Table 35 – Values of Sub-element "error" of messageProtocolHandshakeError	150
188	Table 36 – Structure of SmeConnectionPinStateValue of SME "Pin state" message.	152
189	Table 37 – Structure of SmeConnectionPinInputValue of SME "Pin input" message.....	153
190	Table 38 – Structure of SmeConnectionPinErrorValue of SME "Pin error" message	153
191	Table 39 – Values of Sub-element "error" of connectionPinError.....	159
192	Table 40 – Structure of MessageValue of "data" Message	162
193	Table 41 – Structure of SmeConnectionAccessMethodsRequestValue of SME "Access	
194	methods request" message.....	165
195	Table 42 – Structure of SmeConnectionAccessMethodsValue of SME "Access	
196	methods" message.	166
197	Table 43 – Structure of SmeConnectionCommissioningRequestValue of SME	
198	"commissioning request" message	168
199	Table 44 – Structure of SmeConnectionCommissioningResponseValue of SME	
200	"commissioning response" message	168
201	Table 45 – Structure of SmeConnectionKeyMaterialRequestValue of SME "key material	
202	request" message	169
203	Table 46 – Structure of SmeConnectionKeyMaterialValue of SME "key material"	
204	message.....	170
205	Table 47 – Structure of SmeConnectionKeyMaterialResponseValue of SME "key	
206	material response" message.....	171
207	Table 48 – Structure of SmeConnectionKeyMaterialDeleteValue of SME "key material	
208	delete" message	172
209	Table 49 – Structure of SmeConnectionKeyMaterialDeleteResponseValue of SME "key	
210	material delete response" message	173
211	Table 50 – Structure of SmeConnectionKeyMaterialStateValue of SME "key material	
212	state" message	174
213	Table 51 – Structure of SmeConnectionKeyMaterialStateResponseValue of SME "key	
214	material state response" message	175
215	Table 52 – Structure of SmeConnectionKeyMaterialStateRequestValue of SME "key	
216	material state request" message	175
217	Table 53 – Structure of SmeCloseValue of SME "close" Message.....	176
218	Table 54 – Well-known values for the element "protocolId"	178
219		
220		

221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272

INTERNATIONAL ELECTROTECHNICAL COMMISSION

STANDARD INTERFACE FOR CONNECTING CHARGING POINTS AND/OR CHARGING STATIONS TO LOCAL ENERGY MANAGEMENT SYSTEMS

Part 3: Communication Protocol and Cybersecurity Specific Aspects

For rules on the drafting of the title, refer to the ISO/IEC Directives, Part 2:2021, [Clause 11](#).

The foreword is a mandatory element of the text.

For rules on the drafting of the foreword, refer to the ISO/IEC Directives, Part 2:2021, [Clause 12](#).

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 63380 has been prepared by subcommittee PT63380: Local Charging station management systems, of IEC technical committee 69: Electrical power/energy transfer systems for electrically propelled road vehicles and industrial trucks. It is an International Standard.

The text of this International Standard is based on the following documents:

Draft	Report on voting
-------	------------------

69/878/CD	CC_69_878_CD
-----------	--------------

273
274 Full information on the voting for its approval can be found in the report on voting indicated in
275 the above table.

276 The language used for the development of this International Standard is English.

277 This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in
278 accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available
279 at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are
280 described in greater detail at www.iec.ch/standardsdev/publications.

281 The committee has decided that the contents of this document will remain unchanged until the
282 stability date indicated on the IEC website under webstore.iec.ch in the data related to the
283 specific document. At this date, the document will be

- 284 • reconfirmed,
- 285 • withdrawn,
- 286 • replaced by a revised edition, or
- 287 • amended.

288

iTeh Standards (<https://standards.iteh.ai>) Document Preview

[oSIST prEN IEC 63380-3:2024](https://standards.iteh.ai/catalog/standards/sist/e17457d1-9588-4a9d-937f-4175e5552398/osist-pren-iec-63380-3-2024)

<https://standards.iteh.ai/catalog/standards/sist/e17457d1-9588-4a9d-937f-4175e5552398/osist-pren-iec-63380-3-2024>

289

INTRODUCTION

290 The expansion of renewable energy and the simultaneous reduction in conventional generation
291 result in new power flows and loads on the equipment in the grid and at the house connection
292 point. At the same time, electrical consumers with high power consumption are increasingly
293 being installed in low-voltage systems in private customer systems. These include charging
294 systems for electric vehicles. These two developments can temporarily lead to peak loads and
295 bottlenecks in the network. An expansion of the distribution grids for the comparatively few
296 hours of high simultaneous power consumption is not considered economically sensible. The
297 legislator has therefore introduced the concept of "network-friendly control of controllable
298 consumer devices".

299 It is crucial to define a standardized interface for the connected consumers and generating
300 facilities, which also includes the charging infrastructure for electric vehicles. When developing
301 a local, standardized interface, a fundamental distinction shall be made between the terms
302 power and energy management.

303 In order to avoid an overload and the associated emergency shutdown due to specified power
304 limits in the property while all consumers are drawing electricity at the same time - especially
305 heating and air conditioning technology as well as charging infrastructure - power management
306 is of great urgency. This could allow the maximum load at the grid connection point to be
307 reduced. Accordingly, priority shall be given to local power management over, for example,
308 optimization of operations and tariffs or desired charging plans.

309 In addition to the above-described goal of power management, the further goal of procurement-
310 or tariff-optimized operation can be pursued within the performance limits specified by the
311 infrastructure – controlled by the energy management system. Accordingly, a charging
312 infrastructure will be able to transmit information about procurement and tariff-optimized
313 operation from the local energy management of the property to the electric vehicle so that it
314 can coordinate its charging plan according to local requirements. Effective coordination
315 becomes essential if generating systems (e.g. solar system, combined heat and power plant)
316 are used within the property in order to achieve the highest possible self-consumption of
317 electricity.

318 The long-term goal is to buffer power and energy bottlenecks within a property using the energy
319 stored in the vehicle, which also brings the topic of energy recovery into focus and this aspect
320 needs to be considered during the development of a standardized interface for local power and
321 energy management.

322 The aim of this document is to define a standard interface for connecting charging points and/or
323 charging stations to local energy management systems.

STANDARD INTERFACE FOR CONNECTING CHARGING POINTS AND/OR CHARGING STATIONS TO LOCAL ENERGY MANAGEMENT SYSTEMS

Part 3: Communication Protocol and Cybersecurity Specific Aspects

1 Scope

This IEC 63380 series defines the secure information exchange between local energy management systems and electric vehicle charging stations. The local energy management systems communicate to the charging station controllers via the resource manager.

This IEC 63380 series specifies use cases, the sequences of information exchange, the data models as well as the communication protocols to be used and includes all aspects of local energy management of charging stations.

This IEC 63380 series covers scenarios where the charging infrastructure is managed by the operator of the private electrical network, and local energy management systems are used for local load management.

This IEC 63380 series does not cover the secure information exchange between the charging station and the IT backend system(s), such as the management of energy transfer of the charge session, contractual and billing data, provided by the IT backend.

The IEC 63380 series consists of the following structure, describing the interface between charging stations and local energy management systems.

- Part -1 General Requirements, Use Cases and abstract Messages
- Part -2 Specific Data Model Mapping
- Part -3 Communication Protocol and Cybersecurity Specific Aspects
- Part -4 Test Specifications

This part of IEC 63380 specifies the application of relevant transport protocols; in this case, SPINE (Smart Premises Interoperable Neutral-Message Exchange), SHIP (Smart Home IP), and ECHONET Lite. Other communication protocols can be defined in future editions.

2 Normative references

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

IETF RFC 793, Transmission Control Protocol

IETF RFC 3280 (2002), Internet X.509 Public Key Infrastructure Certificate Revocation List (CRL) Profile

IETF RFC 6455, The WebSocket Protocol

IETF RFC 6763, DNS-Based Service Discovery

ISO/IEC 14543-4-3:2015 Information technology, Home Electronic Systems (HES) architecture — Part 4-3: Application layer interface to lower communications layers for network enhanced control devices of HES Class 1

365 IEC 62394:2022, Service diagnostic interface for consumer electronics products and networks -
366 Implementation for ECHONET

367 IEC 63380-2 CDV: Local Charging station management systems and Local Energy Management
368 Systems network connectivity and information exchange - Part 2: Specific Data Model Mapping

369 **3 Terms, definitions, and abbreviated terms**

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

- 371 • IEC Electropedia: available at <http://www.electropedia.org/>

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

373 **3.1 Terms and definitions**

374 **3.1.1**

375 **CA**

376 **Certificate Authority**

377 **Certification Authority**

378 entity which can provide a digital signature for certificates

379 Note 1 to entry: Other SHIP nodes can check this digital signature with the certificate from the CA itself, the "CA-
380 certificate".

381 **3.1.2**

382 **Commissioning Tool**

383 <SHIP> instrument to establish the trust between different devices in the smart home installation, e.g.,
384 distribute trustworthy credentials from some SHIP nodes to other SHIP nodes

385 Note 1 to entry: E.g., a smart phone, a web server or a dedicated device can embody the role of a commissioning
386 tool. So far, the SHIP specification does not specify a commissioning tool; an interoperable protocol for
387 commissioning can be used on the layer above SHIP.

388 Note 2 to entry: A manufacturer may also use their own solutions

390 **3.1.3**

391 **DNS**

392 Domain Name System,

393 [Source: IETF RFC 1035]

394 **3.1.4**

395 **DNS host name**

396 fully qualified domain name used within DNS as host name to get the IP address of the corresponding
397 internet host.

398 **3.1.5**

399 **DNS-SD**

400 Domain Name System – Service discovery

401 [Source: IETF RFC 6763]

402

403 **3.1.6**

404 **Factory Default**

405 setting that allows the user to reset the SHIP node to the as-new condition; this means that all data that
406 has been provided and stored by the SHIP node during its operation time shall be deleted

407

- 408 **3.1.7**
 409 **IANA**
 410 Internet Assigned Numbers Authority
- 411 **3.1.8**
 412 **IETF**
 413 Internet Engineering Task Force
- 414
 415 **3.1.9**
 416 **IP**
 417 Internet Protocol
- 418 **3.1.10**
 419 **mDNS, multicast DNS host name**
 420 fully qualified domain name used within mDNS as host name to get the IP address of the
 421 corresponding local SHIP node
- 422 **3.1.11**
 423 **M/O/NV/C**
 424 abbreviations which refer to:
- 425 1. M = mandatory
 426 2. O = optional
 427 3. NV = not valid
 428 4. C = choice, i.e., a presence or support depends also on the selection from multiple possibilities
- 429 and which are primarily used within specific definition tables describing certain specialized data model
 430 definitions
- 431 **3.1.12**
 432 **Numerical representation**
 433 written system for expressing numbers. For example, 0xab represents a decimal value of 171
- 434 **3.1.13**
 435 **PIN**
 436 **Personal Identification Number**
 437 specification which makes use of a PIN as secret for SHIP specific verification procedures
- 438 **3.1.14**
 439 **PKI**
 440 Public Key Infrastructure
- 441 **3.1.15**
 442 **Push Button**
 443 switching mechanism to control some aspect of a machine or a process
- 444 Note 1 to entry: A push button event does not necessarily mean that a real physical button has to be used to
 445 trigger this event. A push button event may also be generated by other means, e.g., via a smart phone application
 446 or a web-interface (secure connection to SHIP node required). A push button shall provide a simple mechanism for
 447 a user to bring the device to a certain state or start a certain process.
- 448 **3.1.16**
 449 **QR Code**
 450 the term "QR Code" is a registered trademark of DENSO WAVE INCORPORATED; "QR Code" is the
 451 short form for "Quick Response Code" and used for efficient encoding of data into a small graphic