



DPC: 25 / 30507759 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 09 January 2025

Origin: International

Latest date for receipt of comments: 31 January 2025

Project No. 2025/00158

Responsible committee: PEL/69 Electric vehicles

Interested committees:

Title: BS EN IEC 63119-3 Information exchange for electric vehicle charging roaming service

Part 3: Message structure

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

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

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 31 January 2025**

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

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

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

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

Responsible Committee Secretary: **Ms Andreea Vieru (BSI)**
Direct tel: **0208 996 7432**
E-mail: **andreea.vieru@bsigroup.com**

Introduction

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

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

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

UK Vote

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

Submission of Comments

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

Template for comments and secretariat observations

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

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



69/1031/CD

COMMITTEE DRAFT (CD)

PROJECT NUMBER: IEC 63119-3 ED1	
DATE OF CIRCULATION: 2024-12-20	CLOSING DATE FOR COMMENTS: 2025-02-14
SUPERSEDES DOCUMENTS: 69/942/NP, 69/1024/RVN	

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: SC 23H	HORIZONTAL FUNCTION(S):
ASPECTS CONCERNED:	

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 local regulations or technical reasons that may exist and should be considered should this proposal proceed, recognizing that failure to address such requirements could result in the need for new or existing "In Some Countries" clauses. (SEE [AC/22/2007](#) OR [NEW GUIDANCE DOC](#)).

TITLE: Information exchange for electric vehicle charging roaming service Part 3: Message structure

NOTE FROM TC/SC OFFICERS:

INFORMATION EXCHANGE FOR ELECTRIC VEHICLE CHARGING ROAMING SERVICE

PART 3: MESSAGE STRUCTURE

CONTENTS

information exchange for electric vehicle	1
1. Scope	7
2. Normative Reference	7
3. Terms and Definitions	7
4. Symbols and Abbreviated Terms	9
5. Conventions	10
5.1 OSI Base layer architecture	10
5.2 Requirement structure	10
5.3 Operator ID convention	10
5.4 Common Data type and enumeration	11
5.5 Interface Convention	11
5.4.1 Interface Definition Template	11
5.4.2 Roles of interface	11
5.4.3 Interface working mode	11
5.4.4 Interface Invoking mode	12
5.4.5 Variety convention	12
5.6 Identification Method Type	12
5.7 Unique identifier	13
5.7.1 Requirements of the unique identifier	13
5.7.2 Classification of the global ID	13
5.7.3 Definition of the global identifier	13
6. Information topology	14
6.1 Application service architecture	14
6.2 Application architecture	14
6.3 Information exchange topology	15
6.4 Resource Information	15
6.4.1 information model	15
6.4.2 Typical scenario	16
6.5 Data model compliance	17
7. Transport and format	18
7.1 Protocols Layers	18
7.2 Transport Layer	19
7.3 Session Layer	19
7.4 Presentation Layer	19
7.4.1 JSON message payload encoding	19
7.4.2 Simple value type mapping to JSON	19
7.4.3 Complex value type mapping to JSON	20
7.5 Application Layer	20
7.5.1 Application implementation	20
7.5.2 Interface call method	21

47	7.5.3 Interface call format	21
48	7.5.4 Roaming Message head (REH) specification	21
49	7.5.5 Roaming Message Body (REB) specification	23
50	7.5.5.1 REB-request definition	24
51	7.5.5.2 REB-response definition.....	24
52	7.5.5.3 Message Routing	24
53	7.6 Application Security	25
54	7.6.1 Basic requirement	25
55	7.6.2 Signed Message	25
56	7.7 Platform Authentication Requirements	27
57	7.7.1 basic requirement	27
58	7.7.2 Platform certification model	27
59	7.7.3 Platform authentication methods	27
60	8. Application Layer Data Model	28
61	8.1 General	28
62	8.2 Naming conventions	28
63	8.2.1 Entity	29
64	8.2.2 Element	29
65	8.2.3 Property	29
66	8.2.4 Object	29
67	8.2.5 Key 29	
68	8.2.6 Key path	29
69	8.2.7 Value	30
70	8.2.8 Simple value type	30
71	8.2.9 Complex value type	30
72	8.2.10 Component type	30
73	8.2.11 Message type	30
74	8.3 Events and Activities	30
75	8.4 AttributeType	30
76	8.4.1 ChargingSiteServiceTypeEnum	30
77	8.4.2 ChargingSiteStatusTypeEnum	31
78	8.4.3 ParkingTypeEnum	31
79	8.4.4 ChargingSiteTypeEnum	32
80	8.4.5 ChargingSiteResidentialTypeEnum	32
81	8.4.6 ChargingSitePublicTypeEnum	33
82	8.4.7 ChargingSiteDedicatedTypeEnum	33
83	8.4.8 EVSupplyEquipmentTypeEnum	34
84	8.4.9 EVConnectingPointTypeEnum	34
85	8.4.10 OpreateStatusTypeEnum	35
86	8.4.11 EVSupplyEquipmentStatusTypeEnum	35
87	8.4.12 EVConnectingPointStatusTypeEnum	36
88	8.4.13 ParkingStatusTypeEnum	36
89	8.4.14 LockStatusTypeEnum	36
90	8.4.15 ConnectorInfoTypeEnum	37
91	8.4.16 PaymentTypeEnum	38
92	8.4.17 OperatorWorkingTypeEnum	38
93	8.4.18 TariffDimensionTypeEnum	39
94	8.4.19 SessionTypeEnum	39
95	8.4.20 SessionStatusTypeEnum	39

96	8.4.21 RoleTypeEnum.....	40
97	8.5 Common Object.....	40
98	8.5.1 InfoText Definition.....	40
99	8.5.2 Price Definition.....	40
100	8.5.3 EnergySource Definition.....	41
101	8.6 Public static information Object.....	41
102	8.6.1 Common static Information Object Relations Definition	41
103	8.6.2 Infrastructure operator information (OperatorInfo)	42
104	8.6.3 ChargingSiteInfo	42
105	8.6.4 ChargingStationInfo	44
106	8.6.5 EVSupplyEquipmentInfo.....	44
107	8.6.6 EVConnectingPointInfo	45
108	8.7 Public dynamic information Object.....	45
109	8.7.1 Common dynamic Information Object Relations Definition	45
110	8.7.2 Charging operator status information (operatorStatusInfo)	46
111	8.7.3 Charging site status information (ChargingSiteStatusInfo).....	46
112	8.7.4 Charging terminal status information (ChargingTerminalStatusInfo)	47
113	8.7.5 EVSupplyEquipment status information	
114	(EVSUPPLYEquipmentStatusInfo)	47
115	8.7.6 EVConnectingPoint status information (ConnectingPointStatusInfo)	48
116	8.8 Tariff information Object	48
117	8.8.1 Tariff Information Object Relations Definition	48
118	8.8.2 Tariff information (TariffInfo)	48
119	8.8.3 TariffUnit information (TariffUnitInfo)	49
120	8.9 Session information Object	50
121	8.9.1 Session classification	50
122	8.9.2 Session Information Object Relations Definition	51
123	8.9.3 Service Session information (ServiceSessionInfo)	52
124	8.9.4 EnergyTransferSessions information (EnergyTransferSessionInfo)	52
125	8.9.5 EnergySessionStatus information (EnergySessionInfo)	53
126	8.10 SDR information Object	54
127	8.10.1 SDR Information Object Relations Definition	54
128	8.10.2 SDR information	55
129	8.10.3 EDR data information	56
130	8.10.4 EDR Detail information	57
131	8.10.5 PDR data information	58
132	8.10.6 PDR Detail information.....	58
133	8.10.7 RDR data information	59
134	8.10.8 RDR Detail information.....	60
135	9. Application Layer System Functions.....	60
136	9.1 Roaming Function domain	60
137	9.1.1 General Information Exchange	60
138	9.1.2 Tariff and Pricing.....	61
139	9.1.3 Energy Transfer Management	61
140	9.1.4 Certification Handling	61
141	9.1.5 Support Functions	61
142	9.2 Roaming settlement domain.....	61
143	9.2.1 SDR Reconciliation	61
144	9.2.2 Settlement.....	61

145	9.3 Information interface	61
146	9.4 Information roles about REP	62
147	9.5 System function module implementations per Role	62
148	9.5.1 I3 :Clearing House mode	62
149	9.5.2 I4 : peer to peer mode	63
150	10. Application Layer Message Format	63
151	10.1 General Information Exchange module	63
152	10.1.1 Platform Authentication Token	63
153	10.1.2 Operator Status information query	65
154	10.1.3 Sites information change notify	66
155	10.1.4 Query charging site information	68
156	10.1.5 Dynamic Status of EVSupplyEquipent Change Notify	71
157	10.1.6 Dynamic Status of charging Site Query	72
158	10.2 Tariff and Pricing module	73
159	10.2.1 Inform Home-CSP on tariff information	73
160	10.2.2 Home-CSP request tariffs from Visited-CSO	74
161	10.2.3 Check Home-CSP on tariff information	75
162	10.3 Energy Transfer Management module	75
163	10.3.1 Start charging roaming locally at the charging terminal	75
164	10.3.2 Start charging roaming remotely from Home-CSP	76
165	10.3.3 Start charging roaming remotely from Home-CSP push start	
166	charging results	78
167	10.3.4 Start charging roaming by PnC	79
168	10.3.5 Stop energy transfer session via Home-CSP	81
169	10.3.6 Complete a Charging Service Transaction in a roaming scenario	83
170	10.3.7 query Charging session Information	84
171	10.3.8 Charge Plan Update	85
172	10.3.9 Charge Plan Revoke	86
173	10.3.10 Reservation of an EVSE	87
174	10.3.11 Reservation of a charging Site	89
175	10.3.12 Reservation confirm	90
176	10.3.13 Reservation revoke	91
177	10.3.14 SDR information exchange	92
178	10.3.15 Update Charge Plan by Visited-CSO Credentials Handling	93
179	10.4 Certification Handling module	93
180	10.4.1 Support online identification of the user at a Visited-CSO	93
181	10.4.2 Pre-distribution of Information for Offline Identification of the user	
182	at a Visited-CSO	94
183	10.5 Supporting Functions module	95
184	10.5.1 Maintenance / Outage Information	95
185	10.5.2 Emergency cable unlocking after charging service activated	95
186	10.5.3 Emergency cable unlocking for charging service activation failed	96
187	Annex A Message Code	96
188	Annex A. 1 Error Code	96
189	Annex A. 2 Status Code	97
190	Annex B Security Method	98
191	1.1.1 Data encryption and decryption methods	98
192	1.1.1.1 Data encryption and decryption methods	98
193	1.1.1.2 Example of data encryption and decryption	

194	1.1.2 Signature Method	98
195	1.1.2.1 HMAC-MD5 Parameter Signing Algorithm	98
196	1.1.2.2 HMAC-MD5 Parameter Signing Process	98
197	1.1.3 Secret Key	99
198	1.1.3.1 Secret Key classification	99
199	1.1.3.2 Management of keys	99
200	1.1.3.2.1 Generation of keys	99
201	1.1.3.2.2 Distribution of keys	99
202	1.1.3.3 Use of keys	99
203	1.1.3.3.1 Encryption and decryption of data	99
204	1.1.3.3.2 Parameter signature specification	99
205	Annex C Main Scenario	100
206	Annex C. 1 Scenario1	100
207	Annex C. 2 Scenario2	100
208	Annex D Compatible Evolution	100
209		
210		

1. Scope

This standard describes the process of roaming information exchange between the Home CSP, Visited CSO, and Clearing House through REP. It defines the data structure and messages based on the use cases specified in IEC 63119-2. The roaming endpoint service functions include static and dynamic charging station information exchange, energy transfer service authorization, energy transfer detail record exchange, and remote control commands between each roaming endpoint.

IEC 63119 series do not specify the communication either between Charging Station (CS) and Charging Station Operator (CSO) or between EV and CS.

2. Normative Reference

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

ISO 15118 Road vehicles - Vehicle to grid communication interface all parts of the standard.

CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Reference Architecture. November 2012.

IEC 62559-2 Definition of the templates for use cases, actor list, and requirements list.

IEC 61850-7-420 Basic communication structure - Distributed energy resources logical nodes

3. Terms and Definitions

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

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

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

This clause of Part 1 and Part 2 is applicable except as follows:

Addition:

3.201

service

a series of processes that the service provider provides to the EV user, including energy transfer service, reservation service, parking service, etc.

3.202

service Hub

a series of processes that the service provider provides to connect one or more CPOs to one or more eMSPs.

3.203

chargingSite

.The n

249 **3.204**250 **ChargingTerminal**

251 The physical system where one or more EVs can be charged. A ChargingTerminal has one or more
252 EVSupplyEquipments.Sometimes called Charging Station or Charging Point.

253

254 **3.205**255 **EVSupplyEquipment**

256 equipment or a combination of equipment, providing dedicated functions to supply electric
257 energy from a fixed electrical installation or supply network to **an EV** for the purpose of charging
258 and discharging.

259 **3.206**260 **EVConnectingPoint**

261 terminating point in the fixed installation where energy is transferred to/from one electric vehicle.

262 EXAMPLE A socket-outlet, a vehicle connector or a wireless power transfer device.

263 Note 1 to entry: The connecting point for Modes 1 and 2 is the point where the EV is connected
264 to the supply network.

265 Note 2 to entry: The connecting point for Modes 3 and 4 is the point where one EV is connected
266 to the EV supply equipment

267 Note 3 to entry: The connecting point for Mode 1, Mode 2 and Mode 4, for all plug and cable
268 connected equipment is the standard socket-outlet.

269 Note 4 to entry: The connecting point for Mode 3 and permanently connected Mode 4 is the EV
270 socket-outlet (case A and case B) or the vehicle connector (case C).

271 [SOURCE: IEC 60364-7-722:2018, modified EXAMPLE and Note 1 to entry replaced by Note
272 1 to Note 4]

273 .

274 **3.207**275 **Platform**

276 Software and hardware that provides services via REP. A platform can provide service for a single CSP
277 or CSO.And It can also provide services for both CSP and CSO at the same time.

278 **3.208**279 **Data Demand-er**

280 A technical system role,which calls request to retrieve information from the platform that owns the data.

281 **3.209**282 **Data Owner**

283 A technical system role,which owns information ,can provide data on request call from other platform .

284

285 **3.210**286 **Pull**

287 A system calls request by data demand-er to retrieve information through REP from the data owner.

288 **3.211**

289 **Push**

290 A system calls request by data owner to provide information actively through REP to the data demand-
291 er,in order to update data demand-er platform with latest information.

292

293 **4. Symbols and Abbreviated Terms**

294 PnC plug and charge

295 SOC state of charging

296 PKI public key infrastructure

297 V2G vehicle to grid

298 BMS battery management system

299 SDR service detail record

300 SAC settlement agreement contract

301 SP system platform

302 OID operator identification

303 URI universal resource identification

304 CS charging station

305 CSI charging site

306 CSO charging station operator

307 CSP charge service provider

308 CSZ charging site zone

309 EMAID e-mobility authentication identifier

310 EMOCH e-mobility clearing house

311 EMSP e-mobility service provider

312 EVCC electric vehicle communication controller

313 EVU electric vehicle user

314 ETP energy transfer plan

315 FB functional block

316 FO flexibility operator

317 SA secondary actor

318 SC smart charging

319 SECC supply equipment communication controller

320 TOD time of departure

321 VAT value-added tax
322 URL Uniform Resource Locator

323

324 5. Conventions

325 5.1 OSI Base layer architecture

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

328 This document describes requirements applicable to layer 4 – 7 according to the OSI layered
329 architecture. OSI network communication protocols see table1.

330 **Table 1 – Network communication protocols**

OSI model	Protocol		Function
Application (Layer 7)	I3/I4 Application Layer Message		Define the application service interfaces involved.
	HTTPS	HTTP	Define the distributed, collaborative and hypermedia information based application layer protocols.
Presentation (Layer 6)	JSON		Define the message structure and encoding rules.
Session (Layer 5)	TLS	/	Provide communications' security over the network.
Transport (Layer 4)	TCP		Enable Internet connectivity and process data from applications.

331

332 5.2 Requirement structure

333 This document uses a requirement structure which uses unique identifiers. They mark the
334 individual requirement defined in this document and thereby allow find grained cross references
335 within this document as well as from other parts of the standard.

336

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

338

339

340 **[REP-xx-xxx]** requirement text, where;

341 – 'REP' represents this document.

342 – 'xx' represents a unique marker for a specific clause.

343 – 'xxx' represents a three digit number which is required to be unique within the scope of the
344 associated 'xx' marker. The numbering can be sparse.

345

346 TBD. . .

347

348 5.3 Operator ID convention

349 It is advised to use 63119-2 compliant conventions for Contract IDs and EVSupplyequipment
350 IDs. The home-CSP and visited-CSO name between REPs is important here, to target the right
351 home-CSP or visited-CSO , they need to be known upfront, at least between the cooperating
352 parties.

353

In several case, an issuing authority should be available ,it will manage these central registries of known operators.

5.4 Common Data type and enumeration

In general, all common data types and enumerations are defined inside clause **Error! Reference source not found.** on the "Application layer data model".

Additionally , in some cases where data types and enumerations primarily serve a particular group of messages those data types and enumerations are placed in the clause which defines this group of messages.

5.5 Interface Convention

5.4.1 Interface Definition Template

In general, all common Interfaces are defined inside clause 10 on the "Message Format" follow the Template as table below table 4.

Table 4 - Template of Definitions to interfaces

Template Property name	Template definition
Interface code definition	A code for interfaces' functions designed for indexing and citing. (For example: CSI-000)
Interface endpoint Name	Names of interfaces. For example: Platform Authentication Token.
Interface endpoint Identifier	Service function of interfaces.For example:query_token
Interface Description	The description of this interface functions.
Interface Provider	Provider of data and information.For example: data owner is visited-CSO platform. .
Interface Caller	Demand side of data and information. For example: data demand-er is home-CSP platform
Interface Working mode	The working mode of interface,such as active reporting mode and inquiring mode
Invoking scenarios	The application scenarios description of interfaces.
Invoking mode	The invoking of interfaces,such as condition-invoking mode and schedule-invoking mode

367

5.4.2 Roles of interface

There are two types of technical system roles between REP interface, i.e. interface provider and interface caller.

- The functions of an interface, including providing service entrance, responding to service function request, and returning the execution results of service functions, are implemented by the service interface provider .

- The interface caller makes the service function request and obtains the service function result.Service function request should be executed by interface provider and reply the result.

5.4.3 Interface working mode

There are two types of interface working modes,including active reporting mode and inquiring mode:

- active reporting mode: a data owner should request a call actively to provide data to data demand-er.

- inquiring mode: data demand-er request a call to inquire retrieving data from data owner.

The details of interface working mode can be illustrated by the following table 2.

Table 2 – interface working mode

Working mode	Description	Interface provider	Interface caller
--------------	-------------	--------------------	------------------

active reporting mode	According to the data active update requirement, the data owner request to data demand-er and accomplishes the information active providing and updating .	data demand-er	data owner
inquiring mode	According to the data utility demand, the home-CSP send requests to retrieve data actively from data owner.	data owner	data demand-er

385

386 **5.4.4 Interface Invoking mode**

387 Each REP interface may be called on different invoking mode .Two types of invoking mode
 388 should be involved, i.e. condition-invoking mode and schedule-invoking mode.

389

Table 3 - invoking mode

Invoking Mode	Description	Note
Condition-Invoking mode	The interface would be called/invoked under certain conditions on the basis of the service function demand or certain related factors	The conditions can be categorized as follows: --The interface would be called when an instant inquiry request is launched by the user. --The interface would be called when a service warning event was detected.
Schedule-Invoking mode	The interface would be called/invoked periodically on the basis of the service function demand .	The interface may invoked by schedule and the triggering frequency is generally set according to the default system parameter and can be adjusted if necessary.

390

391

392 **5.4.5 Variety convention**

393 To prevent issues with capitals in variable names, the naming in JSON is not CamelCase but snake_case.
 394 All variables are lowercase and include an underscore for a whitespace.

395 **5.6 Identification Method Type**

396 All the identification methods sFCh as Apps, RFID, PnC, etc. which are used by the roaming
 397 endpoint may be generally defined as below:

398

399 -Apps.

400 Identification mode where the EV user provides the EVSE ID and contract information by the
 401 mobile device through the internet before plugging the vehicle .

402 - RFID.

403 Identification mode where the EV user provides the contract information by swiping the RFID
 404 card before plugging the vehicle.

405 - PnC.

406 Identification mode where all aspects of charging are automatically taken care of with no further
 407 intervention from the EV user. For example,

- 408 • Type1 PnC=ISO 15118 PnC
- 409 • Type2 PnC=GBT PnC

410 5.7 Unique identifier

411 5.7.1 Requirements of the unique identifier

412 To achieve the roaming between the different platforms, the following requirements shall be
413 fulfilled:

- 414 • All the identification such as REP ID, equipment ID, connector ID, energy transfer
415 transaction ID, etc., which are used by roaming endpoint shall be universally unified and
416 unique All the identification such as REP ID, equipment ID, connector ID, energy
417 transfer transaction ID, etc., which are used by roaming endpoint shall be universally
418 unified and unique
- 419 • The identification field should consist of two parts: global and local
- 420 • The global part of the identification shall be public and unique
- 421 • The local part of the identification shall be defined and managed respectively by
422 CSP/CSO
- 423 • The information routing and destination addressing shall be realized by distinguishing
424 the global part of the ID during the information exchange for roaming

425 5.7.2 Classification of the global ID

426 The global identifiers used by the roaming endpoint are classified as follows:

427 - REP ID

428 The unique ID of the CSP/CSO/CH which implements the roaming endpoint

429 - Equipment ID

430 The unique ID of the dedicate equipment or charging station owned by roaming CSP/CSO

431 - EVSE ID (connector ID)

432 The unique ID of the EV supply equipment or connector owned by roaming CSP/CSO.

433 - energy transfer transaction ID.

434 the unique number of the roaming energy transfer transaction .

435 5.7.3 Definition of the global identifier

436 The global identifier shall adopt envelope schema. Encapsulate the original protocol issuer ID,
437 original format ID and original ID.

438 Table 1 - Structure of the global identifier

Format Issuer ID	Format ID	Original ID (local ID)
4 Bytes (ALPHA / DIGIT)	4 Bytes (ALPHA / DIGIT)	(ALPHA / DIGIT)
NOTE 1 ALPHA is the element of [%x41-5A / %x61-7A]; according to RFC 5234 (7-Bit ASCII)); a-z/A-Z NOTE 2 DIGIT is the element of [%x30-39]; according to RFC 5234 (7-Bit ASCII));0-9 NOTE 3 Alpha characters shall be interpreted case-insensitively.		

439 Each section is defined in Table 3

Table 2 - Definition of the global identifier syntax

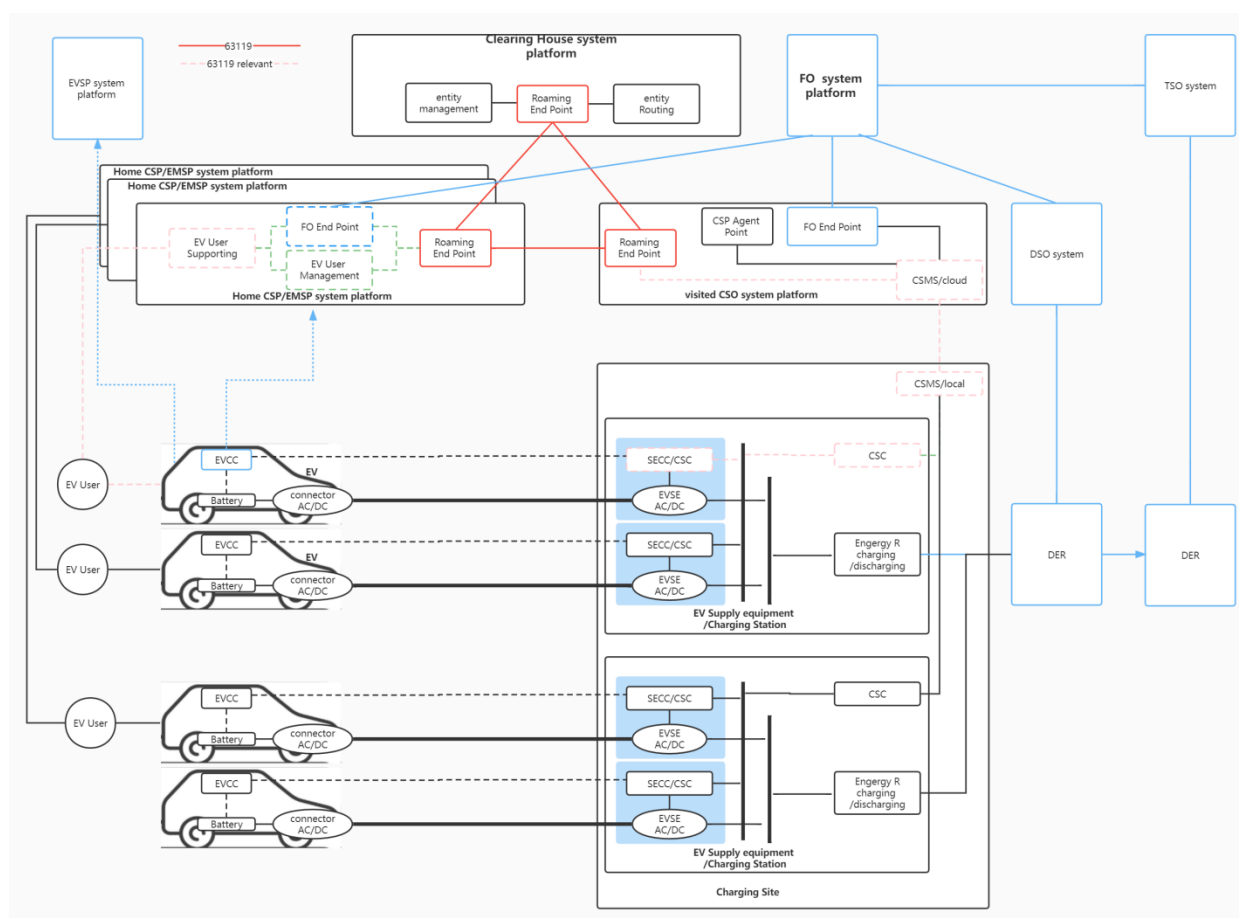
Section	Definition
Format Issuer ID	indicating which protocol issuer format the encapsulated protocol - "GBT" indicates CN protocol - "EMI" indicates EMI3 format
Format ID	referring to the version number of the current protocol, defined by the protocol issuer
original Identifier (local Identifier)	alphanumeric characters, referring to the original ID (local ID) sFCh as GBT ID, EMI3 ID

6. Information topology

6.1 Application service architecture

Application service architecture see diagram 1.

Diagram 1 – Application service architecture



6.2 Application architecture

There exist many topological communication solutions for charging roaming service.:

- EVUser--->Home-CSP App--->Home-CSP platform--->visited-CSO platform-->EVSupplyEquipment--->EV

- EVUser--->FO--->Home-CSP App--->Home-CSP platform--->visited-CSO platform-->EVSupplyEquipment--->EV
- EVUser--->FO--->Home-CSP App--->Home-CSP platform--->Clearing House platform -->visited-CSO platform--->EVSupplyEquipment--->EV

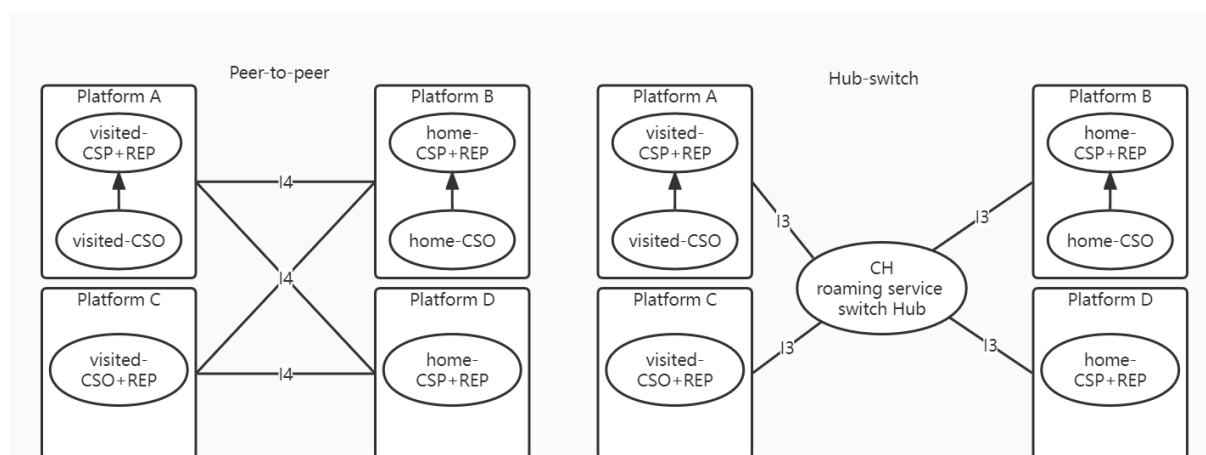
6.3 Information exchange topology

There exist two topological communication solutions for charging roaming service. One is the topology solution of Hub collection, where the interface service is defined as I3 interface protocol, and the other is the peer-to-peer topology solution, where the interface service is defined as I4 interface protocol.

- peer-to-peer topology: This topology is a bilateral connection between two platforms, and both platforms have multiple different and also the same roles.
- Hub-switch topology: This topology is multiple bilateral connection between multiple platforms, and each platform has multiple different and also the same roles.

See the diagram 3 below.

Diagram 3 – Information exchange topology



EV Charging roaming service is achieved through the interaction of information between platforms. With Message Routing functionality it also becomes possible to support Platforms that host multiple roles. A lot of parties are not only CSO or CSP/eMSP. Most are both CSO and CSP/eMSP. The platforms involved in charging roaming service fall into four categories:

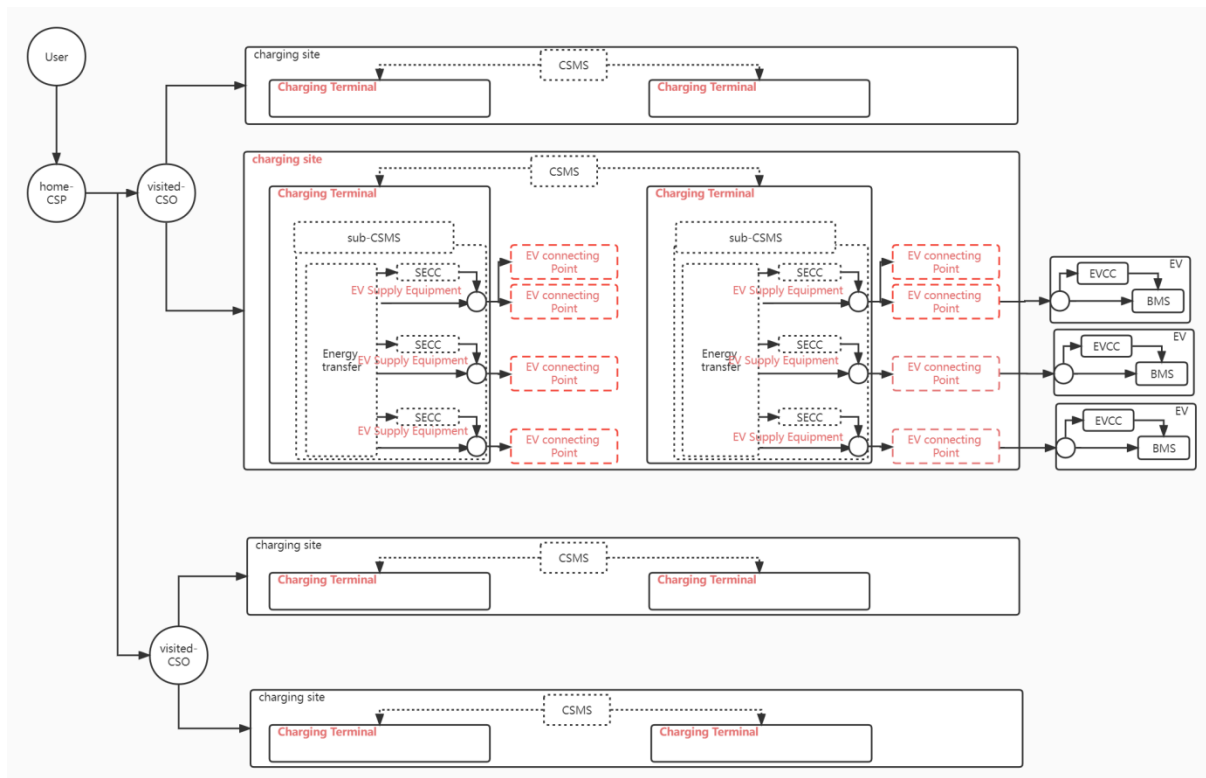
- Platform A: Some visited parties have multiple roles, including CSP role and CSO role, and CSP integrates CSO function and REP function.
- Platform B: Some home parties have multiple roles, including CSP role and CSO role, and CSP integrates CSO function and REP function.
- Platform C: Some visited parties have one CSO role, and provide visited-CSO function and REP function.
- Platform D: Some home parties have one CSP role, and provide home-CSP function and REP function.

6.4 Resource Information

6.4.1 information model

The information model is an abstraction of the actual physical scenario. It consists of the CSO service network, ChargingSite, Chargingterminal, EVSupplyEquipment, and connecting point. See the diagram 3 below.

Diagram3 – Information model



The energy transform information topology, as relevant to the CSP, consists of five entities:

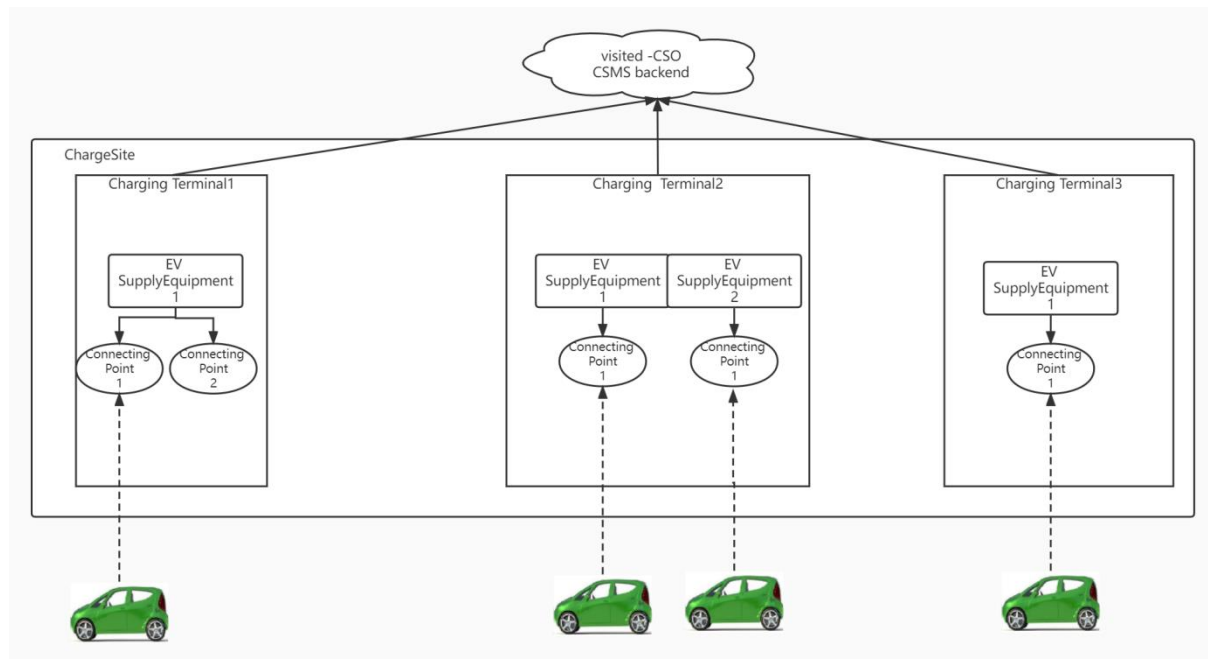
The entities relationship may be described as below:

- A CSO service network object has a list of ChargingSites.
- A ChargingSite object has a list of Chargeterminals. ChargingSite is a group of one or more Chargeterminals that belong together geographically or spatially. A ChargingSite is typically the exact location of one or more Chargeterminals, but it can also be the entrance of a parking garage or a gated community. It is up to the CSO to use whatever makes the most sense in a specific situation. Once arrived at the location, any further instructions to reach the Chargeterminals from the ChargingSite are stored in the Chargeterminals object itself.
- A Chargingterminal object has a list of EVSupplyEquipments
- A EVSupplyEquipment object has a list of connectingpoints which can not be used simultaneously, only one connectingpoint per EVSupplyEquipment can be used at the time. EVSupplyEquipment is the part that controls the power supply to a single EV in a single session. An EVSupplyEquipment may provide multiple connecting points but only one of these can be active at the same time.
- A EV connecting point is a specific socket or cable available for the EV to make use of.

6.4.2 Typical scenario

The data model can be used in three typical scenario applications. See the diagram 5 below.

Diagram5 – data model application scenario

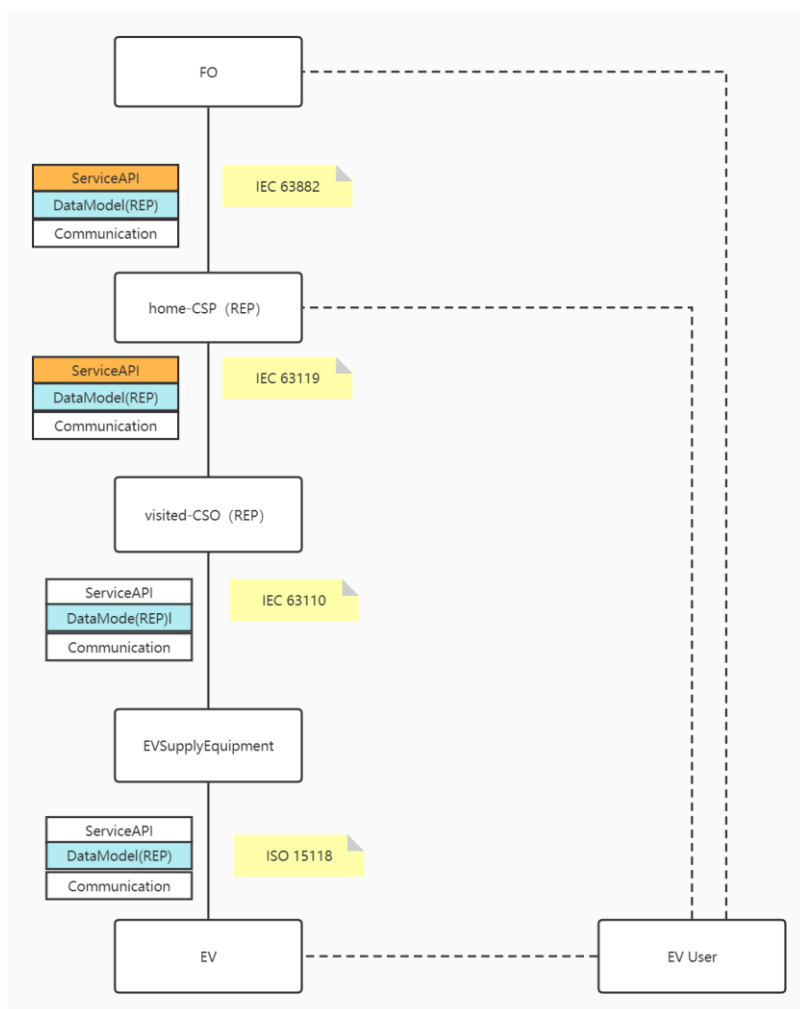


According to diagram 5 typical scenario ,the energy transport ability may be described as below:

- Charging terminal 1 consists of an energy exchange system with two adaptable connectors, such as CCS1 and CHAdeMO, which can only serve one vehicle at a time .Otherwise ,it can provide information to guide the vehicles which has any of adaptable connectors to charging when it is in idle.
- Charging terminal 2 consists of two energy exchange system with each adaptable connectors, which can serve two vehicle at a time .And,it can provide information to guide two vehicles coming to charge .
- Charging terminal 3 consists of an energy exchange system with one adaptable connectors, which can only serve one vehicle at a time.And,it can provide information to guide two vehicles coming to charge .

6.5 Data model compliance

	IEC/ISO15118	IEC63110	IEC63119	IEC63882
OperatorInfo			be	be
ChargingSite			be	be
ChargingTerminal		be	be	
EVSupplyEuipment	be	be	be	be
EVConnectingPoint	be	be	be	



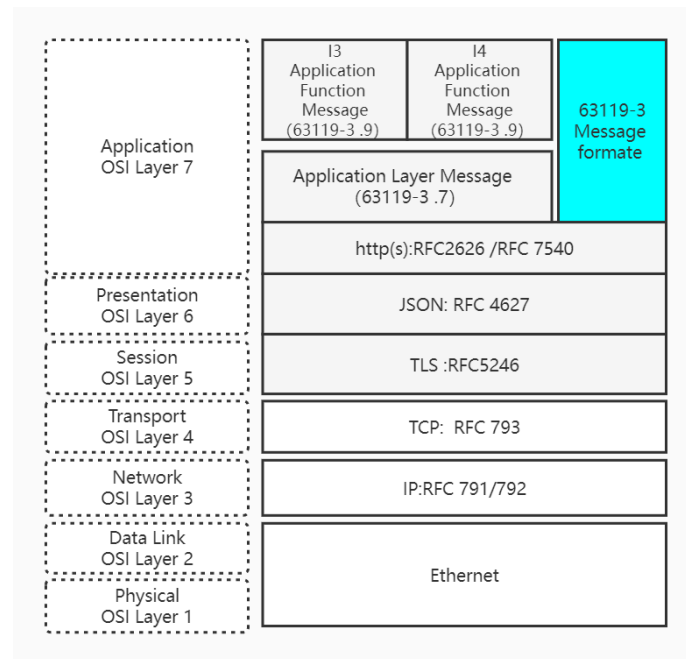
7. Transport and format

This section presents the general requirements that implement of the roaming protocol.

7.1 Protocols Layers

Application protocols see diagram 6.

Diagram 6 – Application protocols



7.2 Transport Layer

The transport layer uses TCP ,referring to RFC793,to guarantee the connectivity of the network for all parties involved in the exchange of information.

7.3 Session Layer

The TLS protocol is defined at the session layer to create a secure connection between two applications over the network, preventing eavesdropping and tampering during the exchange of data.TLS protocol is uncoupled from higher-level application layer protocols such as HTTP. Application layer protocols can run transparently on top of the TLS protocol, and the TLS protocol performs the negotiation and authentication required to create an encrypted channel. Data transmitted by the application layer protocols is encrypted as it passes through the TLS protocol, thus ensuring the privacy of the communication.

7.4 Presentation Layer

The presentation layer refers to the technology which is used to encode the actual information contained in the complex value types which define the application layer messages.

According to application layer messages the payload defined by the presentation layer is wrapped in additional envelopes which among other things provide capabilities like payload versioning, message routing or compression.

7.4.1 JSON message payload encoding

The presentation layer of IEC 63119-3 shall use JSON according to IETF RFC 8259 for the encoding of application layer messages.

7.4.2 Simple value type mapping to JSON

The following table defines which JSON representation shall be used in order to encode the values of which simple value type.

Simple value type	JSON type	Description
NullType	literal	The literal value 'null' .
BooleanType	literal	One of the two literal values: 'true' or 'false' .

UnsignedInteger8Type	number	An unsigned numeric value with only an integer part.
UnsignedInteger16Type	number	An unsigned numeric value with only an integer part.
UnsignedInteger32Type	number	An unsigned numeric value with only an integer part.
UnsignedInteger64Type	number	An unsigned numeric value with only an integer part.
SignedInteger8Type	number	A signed numeric value with only an integer part.
SignedInteger16Type	number	A signed numeric value with only an integer part.
SignedInteger32Type	number	A signed numeric value with only an integer part.
SignedInteger64Type	number	A signed numeric value with only an integer part.
Float32Type	number	A signed numeric value which may also contain a fraction part and/or an exponent part.
Float64Type	number	A signed numeric value which may also contain a fraction part and/or an exponent part.
StringType	string	A Unicode string.
OctetStringType	string	A string containing a Base64 encoded representation of the octet data sequence.
TimestampType	string	A string containing a Base64 encoded representation of the octet data sequence

560

561 **7.4.3 Complex value type mapping to JSON**

562 Values of properties which have been declared with a maximum cardinality larger than ‘1’
563 shall always be encoded at the presentation layer inside a JSON array structure.] Values of
564 properties which have been declared as Any ComplexValueType or any of its subtypes shall be
565 encoded at the presentation layer as a JSON object structure where each member encodes one
566 property of the complex value.

567 **7.5 Application Layer**568 **7.5.1 Application implementation**

569 All REP interfaces shall be of HTTP(S) interfaces, with the URL of each interface defined as
570 the following format.

571

572 **http(s)://[domain]/roaming/v[version-number]/[interface-endpoint]**

573

574 a)[domain]: domain name, refer to operator platform web service domain name.

575 b) [version-number]: represents the service interface version number. Different version
576 addresses correspond to the corresponding version code. During a system upgrade session, the
577 old and new versions may exist at the same time, and the old version of the service interface would
578 be offline when all interaction parties have adopted the new version interface, which helps the user
579 experience to upgrade seamlessly.

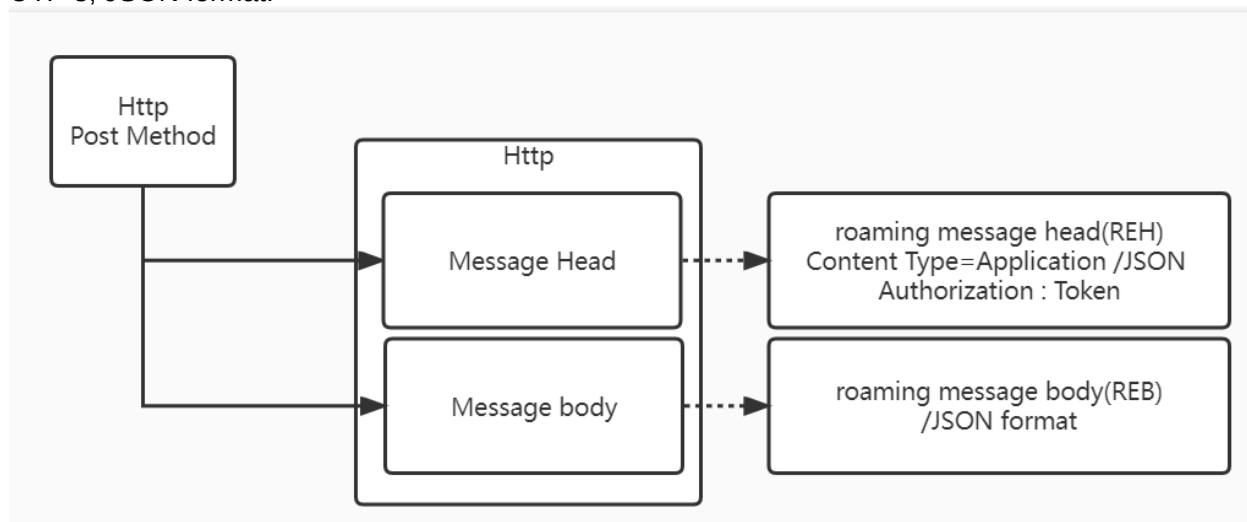
c) [Interface-endpoint]: The name of the requested/invoked service interface, referring to different service functions. To ensure that the functions of each interface are clear and unambiguous, only one service function is allowed per URL.

7.5.2 Interface call method

The request method should be POST call method . The protocol uses them in a way similar to REST APIs.

7.5.3 Interface call format

The interfaces shall all use HTTP(S)/POST to provide parameters in JSON format, and the request shall contain both the message header and the message body. The data shall be encapsulated in UTF-8, JSON format.



7.5.4 Roaming Message head (REH) specification

1. Content -type

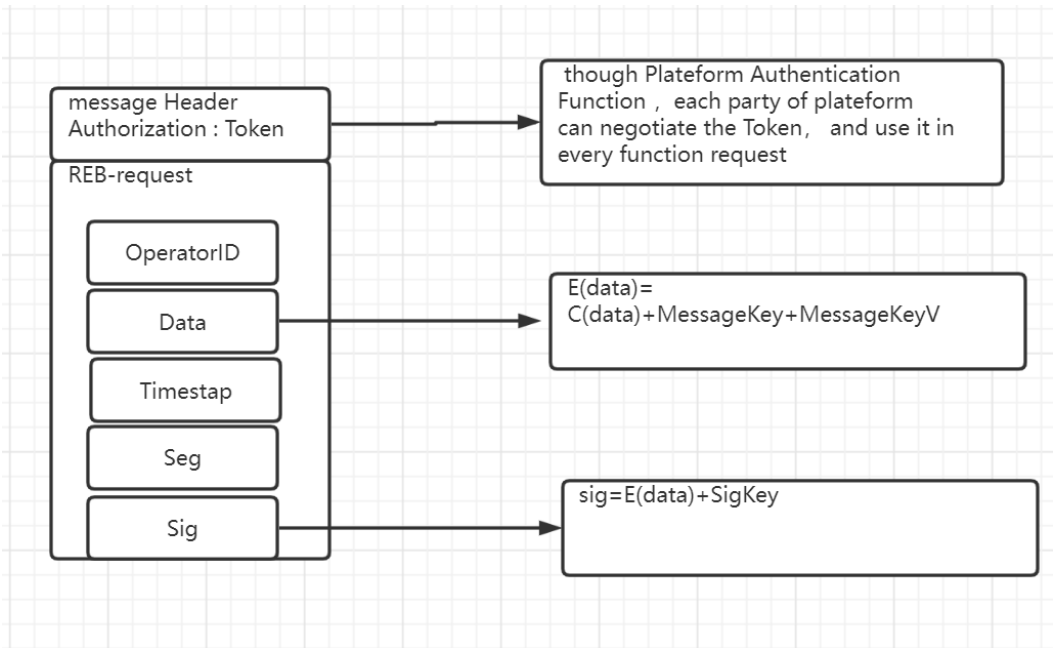
The HTTP message header: Content-Type SHALL be set to “application/json” for any request that contains a message body.

The Content-Type field is used to identify the encoding method of the message body in the request. The information exchanged in this standard shall be in the form of JSON, and the parameter information shall be encoded in UTF-8.

2. Authorization Token

The message header generally shall define the content type and authorization information (Authorization).

The Authorization field is used to prove that the client has permission to access the resource. The authorization information specified in this standard is in the form of a token, so the authorization in the configuration message header must be a bearer token.



605

606 3. Authorization Token Specification

607 Authorization Token follow Json web token (JWT) as Specification. A JSON-based open standard
608 for passing declarations between web application environments ((RFC 7519). JWT declarations
609 are generally used to pass authenticated user identity information between identity providers and
610 service providers to facilitate access to resources from resource servers, and to add additional
611 declarations necessary for other business logic. The token can also be used directly for
612 authentication, or it can be encrypted.

613 4. Authorization Token format

614 The REH Authorization Token follows the JWT format and is made up of three parts, i.e., the
615 header, the payload and the signature. Three parts should be converged by symbol ".".
616

header	.	payload	.	signature
--------	---	---------	---	-----------

617

618 1) header

619 The header of the JWT contains two major parts of information

620 Declaring the type, which is JWT.

621 Declaring the encryption algorithm, which is generally HMAC SHA256.

622 An example of header:

623 {
624 'typ': 'JWT',
625 'alg': 'HS256'
626 }

627 Then the base 64 encryption is applied to header.

628 2)payload

629 The payload is the part where the information is stored, which contains three parts:

630 Registered Claim Names.

631 Public Claim Names.

632 Private Claim Names.

633 A) Declaration of the registration in the standard

634 iss: The "iss" (issuer) claim identifies the principal that issued the JWT.

635 sub: The "sub" (subject) claim identifies the principal that is the subject of the JWT.

636 aud: The "aud" (audience) claim identifies the recipients that the JWT is intended for.

637 exp: The "exp" (expiration time) claim identifies the expiration time on or after which the JWT must not be
638 accepted for processing.

639 nbf: claim identifies the time before which the JWT must not be accepted for processing.

640 iat: The "iat" (issued at) claim identifies the time at which the JWT was issued.

641 jti: The "jti" (JWT ID) claim provides a unique identifier for the JWT.

642 B)Public Claim names:

643 Claim Names can be defined at will by those using JWTs. The definer of the name or value needs to take
644 reasonable precautions to make sure they are in control of the part of the namespace they use to define the
645 Claim Name.

646 C) Private Claim Names

647 A producer and consumer of a JWT MAY agree to use Claim Names that are Private Names: names that are
648 not Registered Claim Names or Public Claim Names.

649 Example of a payload:

```
650 {
651   "sub": "REP-01",
652   "name": "CSO",
653   "admin": true
654   iat: '2022-09-22'
655 }
```

656 Then Base64 encoding is applied to encode the second part of JWT.

657

658 3)the third part of JWT contains signature information, which includes:

659 header (before been encrypted by base64)

660 payload (after been encrypted by base64)

661 Secret

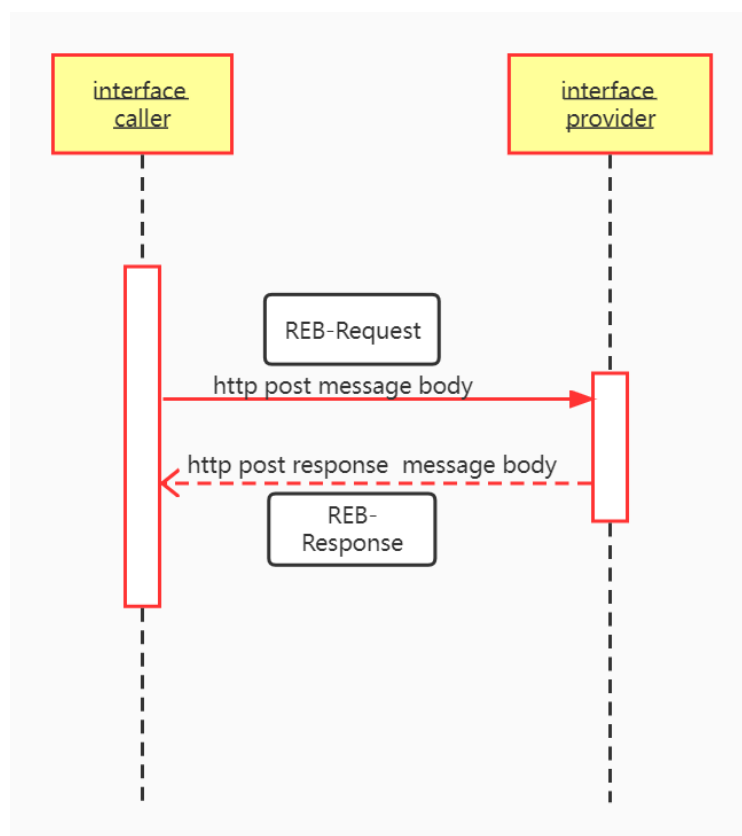
662 The string, which is formed by connecting the base64 encrypted header and payload with connector
663 “.”, will be **encrypted** with the encryption method mentioned in the header, which generates the third
664 part of JWT.

665 By connecting the above three parts with a connector “.” to generate a string, the JSON web token
666 would be formed.

667

668 7.5.5 Roaming Message Body (REB) specification

669 REB consist of two message body definition: REB-request and REB-response.



670

671

7.5.5.1 REB-request definition

REB-request message body generally consists of five parameter fields, include OperatorID, Data, TimeStamp, Seq, and Sig, as specified in Table 2.

Table 2 – Message body content table

Parameter Name	Parameter Description
to-country-code	'country code' of the connected party this message is to be sent to.
to-REP-ID	'REP-ID' of the connected party this message is to be sent to.
from-country-code	'country code' of the connected party this message is sent from.
from-REP ID	Operator system platform REP identification code of the message requestor platform. For example :one CSO system platform is "ABCDEFGHI"
Enable-Data-encryption	"True" "false"
Data	Specific information for each function .The Data field in the Data Transfer Interface can be in an array type JSON format, through which the data sender can transfer bulk data. It is a encryption data ,which encryption key is issued by response service ,if Enable-Data-encryption is set to "true"
TimeStamp	Timestamps are used to mark the time characteristics of messages For example : " yyyyMMddHHmmssXXXX"
Seq	self-incrementing sequence number is used to avoid message duplication during message interaction process. For example : "0010110011"
Sig	Parameter Signature allows the receiver of the message to confirm the source of the data and the integrity of the data ,to protect the message from illegal changing by attackers . For example : "0010110011"

7.5.5.2 REB-response definition

REB-response message body generally consists of five parameter fields, include Ret ,Msg, Data, and Sig, as specified in Table 3

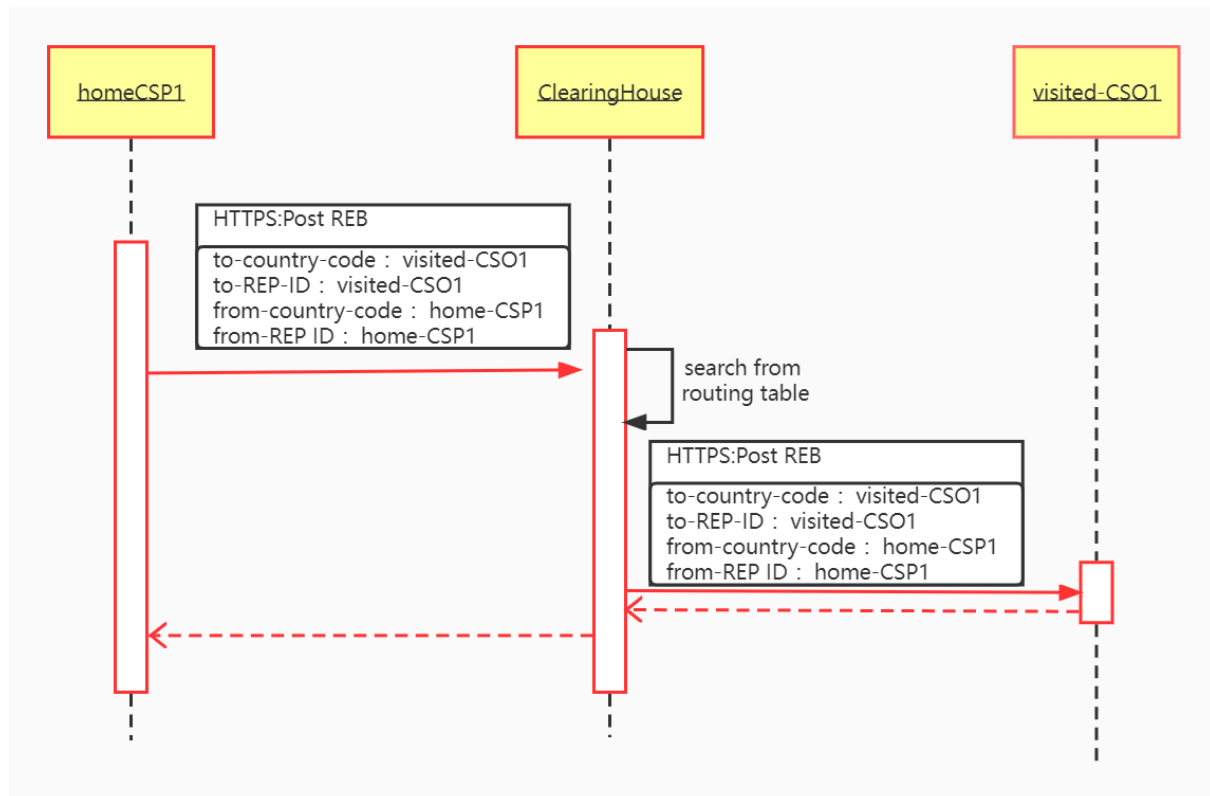
Table 3 – Message body content table

Parameter Name	Parameter Description
Ret	the result parameter code , code list see annex . For example : "10014001"
Msg	the result description by response service
Data	Specific information for each function, It is a encryption data ,which encryption key is issued by response service
Sig	Parameter Signature allows the receiver of the message to confirm the source of the data and the integrity of the data ,to protect the message from illegal changing by attackers . For example : "0010110011"

7.5.5.3 Message Routing

When REP is used to communicate to/from a Platform or via a Hub the following four HTTP headers are to be added to any request/response to allow messages to be routed.

When implementing these four headers SHALL be implemented for any request/response to/from a Functional Module. This does not mean they have to be present in all request.



688
689

690 7.6 Application Security

691 7.6.1 Basic requirement

692 The operator should comply with the requirements of ISO/IEC 27001 on data security transmission
693 control.

694 The operator shall provide a strict system security and confidentiality mechanism to guarantee the
695 safe, stable and reliable operation of the information exchange interface, including the access
696 control of information and the security of application system operation.

697 Cryptographic algorithms shall be used for security functions such as key generation, distribution,
698 HMAC, and encryption. The associated algorithm modules should not be modified or exported
699 outside the secure environment during their lifecycle.

700 The key for the specified function shall be used only for the specified function.

701 7.6.2 Signed Message

702 For certain architectures it can be useful to use signed application messages. This gives the visited-
703 CSO and home-CSP the ability to guarantee that messages are sent by the other party. For
704 example when a visited-CSO is involved, the Clearing House or home-CSP can know that a
705 message received from the visited-CSO is created and signed by the visited-CSO.

706
707 Because message signing is needed in all architectures and scenarios, it is required for all REP
708 implementations. It will depend on the security requirements if this is required.

709
710 This section defines a method to digitally sign any REP message. For each normal REP message
711 an equivalent signed message is defined that encapsulates the normal message, and adds a digital
712 signature.

713 1. Signed Message Format

714 For Signed REP Messages, JWS is used. For more information see: [RFC7515].

715 Suppose visited-CSO have an REP calls encoded in the REP message:

716

717 [`<MessageTypeId>`, "`<MessageId>`", {`<Extension>`}, "`<Action>`", {`<Payload>`}]

718 Then we define the equivalent signed message as follows.

[<MessageType>, "<MessageId>", {<Extension>}, "<SignedAction>", {<SignedPayload>}]

The <MessageType> and <MessageId> SHALL stay the same. The <SignedAction> field SHALL be the action name (<Action>) with the string "-Signed" appended. For instance, if "<Action>" is "BootNotification", then "<SignedAction>" is "BootNotification-Signed". The <SignedPayload> SHALL be the JWS encoding of the payload, computed according to the following settings:

The JWS Payload SHALL be the <Payload> from the original message.

The JWS Protected Header SHALL contain a field called "REPACTION" containing the name (<Action>) of the OCPP action, and a field called "REPMessageTypeId" containing the message ID (<MessageType>).

The JWS Protected Header SHOULD contain the x5t#S256 field to identify the key used for signing, as specified in Section 7.4.

The <SignedPayload> SHALL be encoded using the Flattened JWS JSON Serialization syntax.

2. Handling Signed Messages

When a home-CSP receives a signed message, it SHALL extract the encapsulated normal message. It SHALL process it normally, following the 63119-3 standard. It MAY perform additional actions that use the digital signature. This is optional, because a secure connection between the home-CSP and the visited-CSO is expected, hence a second process to validate a signature on message level is redundant. When a visited-CSO receives a signed request, and it supports digital signing, it SHALL send a signed reply.

3. Allowed Algorithms

The algorithms allowed for use with JSON Web Signatures are defined in the JSON Web Algorithms standard [RFC7518]. To limit the cryptographic algorithms that a Charging Station has to implement, for REP the same algorithms SHALL be used as for the TLS connection used to secure communications. This means that for generating the digital signatures, the visite-CSO and home-CSP use the following algorithms from the JSON Web Algorithms standard [RFC7518], section 3.1:

- ES256: ECDSA using P-256 and SHA-256
- RS256: RSASSA-PKCS1-v1_5 using SHA-256
- RS384: RSASSA-PKCS1-v1_5 using SHA-384

Note that RS256 and ES256 are the algorithms recommended by [\[RFC7518\]](#).

4. Key management

This section does not prescribe specific keys to be used for digital signatures. The CSMS visite-CSO and home-CSP Certificate, used for setting up a secure TLS connection, MAY be used for signing. For many use cases, these will however not be the correct keys. For instance, if the use case is to provide non-repudiation of meter readings, the messages should be signed with a certificate stored in the calibrated measuring chip.

To be able to verify the digital signature, one needs to know which key was used to sign it. JSON Web Signatures supports several ways to store a key identifier with the signed message. As the certificates that can be used for signing are not specified, hash values will be used to identify them. Within the REP, the visite-CSO and home-CSP SHOULD include the field x5t#S256 in the JWS Protected Header to identify the certificate. Following the JSON Web Signatures standard [RFC7515] the value of this field SHOULD be set to the SHA-256 hash of

the DER encoding of the signing certificate. How stakeholders can look up the certificate based on the hash value is out of scope for this document.

7.7 Platform Authentication Requirements

EV energy transferring information exchange should comply with the requirements of ISO27001 on session connection, which generally requires platform authentication, request and answer

7.7.1 basic requirement

The exchange of information on electric vehicle charging and switching services shall comply with information security protection requirements.

Electric vehicle charging roaming service should have a platform authentication service for information exchange. Only after authentication success, information exchange can be implemented between the platforms.

The operator shall provide a strict system security and confidentiality mechanism to guarantee the safe, stable and reliable operation of the information exchange interface, including the access control of information and the security of application system operation. Basic requirements including:

- a) Security measures such as authentication, access control, data encryption, digital signatures, etc..
- b) The use of secure, reliable and commonly used encryption algorithms.
- c) The storage of keys and the encryption/decryption of transaction information need to be in a secure environment.
- d) Key updates and activation should be possible on a regular basis or in response to bursts.
- e) Provide a mechanism for source correctness identification of messages (HMAC)

7.7.2 Platform certification model

Platform authentication shall support either distributed authentication mode or central exchange authentication mode .

Distributed authentication mode means each operator needs to authenticate by itself, and the specific authentication method can be negotiated by the operators. The central exchange authentication mode means there shall be a unified authentication service provider which undertakes all the platform authentication services, and the specific authentication method needs to be agreed by all the operators and the authentication service provider.

7.7.3 Platform authentication methods

It is advisable to adopt a combination of identity authentication and access control for platform authentication, and see Fig 5-2 for the relevant process.

Authentication can take the form such as user name/password authentication, key authentication or digital certificate authentication; access control can take a combination of IP access control, time access control and other methods.

Token shall be granted after user authentication succeeds. Each request from the server side should carry the Token issued by the server side. The server side shall verify the Token first. Only verification succeed, then the client side responds with the requested data. The validity period of the Token is determined by the service provider and should not exceed a maximum of 7 days. Authentication service should be re-initiated if the Token is lost or invalidated. See Appendix A for the authentication interface specification.

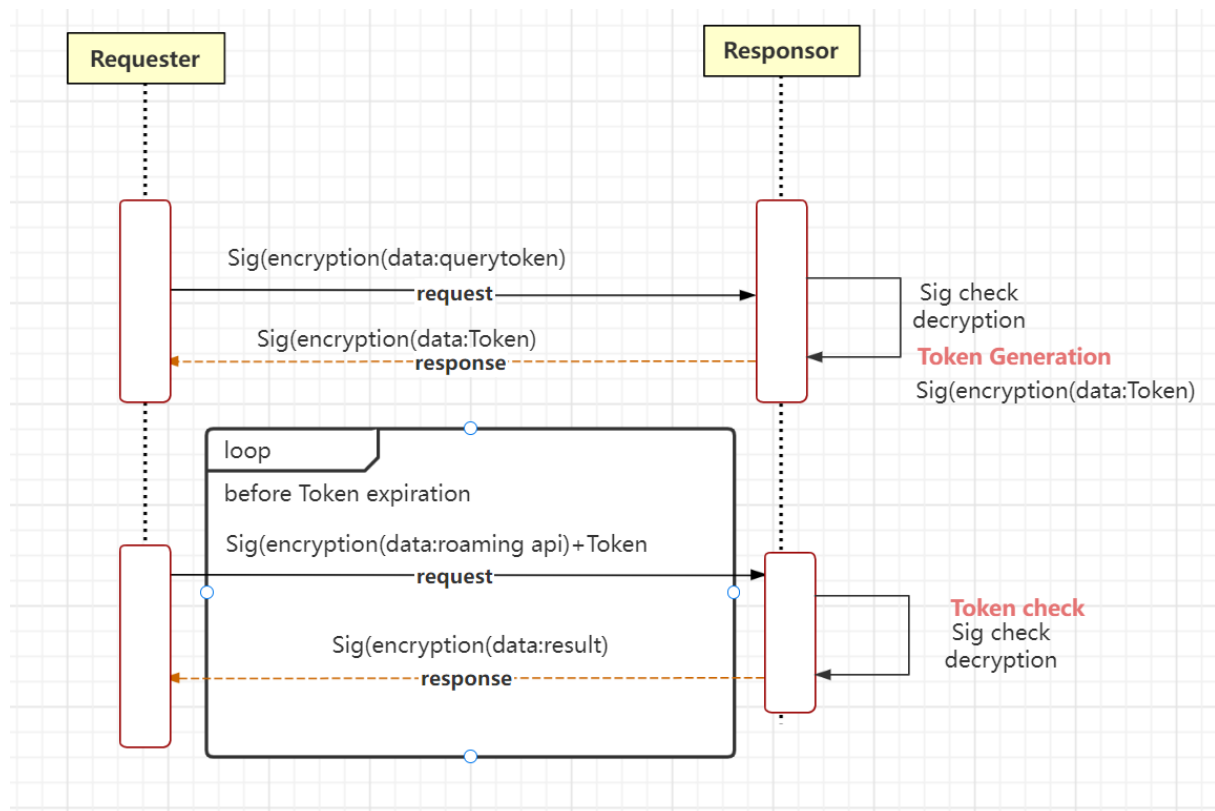


Diagram 1 Platform authentication method

8. Application Layer Data Model

8.1 General

8.2 Naming conventions

This standard has chosen a number of naming rules for the technical identifiers (keys) which are defined and used in the following clauses and which also shall be followed when non-standard extensions (namespaces) get defined.

There are a number of design goals which have been taken into account when forming those conventions and requirements:

- Reduce the complexity when implementing this standard in common programming languages.
- Reduce the need of key mapping when storing 63119 objects in common database systems.
- Ensure easy mapping of 63119 Properties to other protocols or computer monitoring tools.
- Ensure proper support for future expandability.

While many of the important terms already have been introduced in clause on "Terms and definitions" and some will also be described in full detail in a dedicated clause, it is necessary to provide some more background to them here already. Those terms will be used very frequently in the remaining clauses to describe the object model, the message interactions as well as the requirements related to naming conventions.

840 NOTE: In the context of this clause the phrase "ASCII code" refers to the codes defined in ISO
841 8859-1.

842 8.2.1 Entity

843 *Entities* are an abstract concept which tries to classify a specific and complete pattern, that will
844 be applied (reused) whenever an object which matches that *Entity* pattern needs to be described.
845 *Entities* are typically building on top of the definition of other *Entities*.

846 Each *Entity* always represents (includes) all embedded patterns, down to every last leaf
847 *Property*. In that sense *Entities* are different from complex value types, because complex value
848 types only represent a very isolated slice of the entire *Property* tree which represents an *Entity*
849 pattern. So while technically, *Entities* get described with the help of complex value types, a
850 complex value type is not equivalent to an *Entity*.

851 NOTE: In programming languages *Entities* are often referred to as classes, and classes are
852 typically described with the help of structures.

853 8.2.2 Element

854 Elements contain values. The values which elements enclose or contain can either be a simple
855 value type or a group of other child elements, which form or follow the pattern of a complex
856 value type.

857 Elements are identified in the context of their parent element with the help of a key, which in
858 that context turns them into a concrete object *Property*.

859 NOTE: In the XML encoding standard the term "element" has a very precise definition. Since
860 this standard uses XML at the XMPP transport layer the definitions of the object model
861 intentionally avoid the term element, unless it actually refers to the XML concept.

862 8.2.3 Property

863 Properties get uniquely identified within the context of an abstract complex value type by a key.
864 In the abstract form properties define their value type as well as default access rules. They are
865 the first level child elements of an enclosing parent element.

866 In the concrete form *Properties* also hold the simple or complex values of concrete objects.

867 8.2.4 Object

868 The term object describes a concrete incarnation of an *Entity*. In contrast to *Entities*, the objects
869 are not just a pattern, but they have concrete values associated with their *Properties*.

870 Objects are typically nested complex value type structures, and an object is defined by the
871 entirety of all its child *Properties* up to the very last leaf *Properties*, which are always holding
872 values of a simple value type. The *Properties* of an object are very often objects themselves.

873 8.2.5 Key

874 A key is a name that uniquely identifies a *Property*, and thereby its associated value. Keys
875 conceptually are the reference to the local address of a value.

876 Keys are required to be unique within the same scope, for example a specific complex value
877 type. However, this document also defines keys which, based on the naming convention,
878 guarantee uniqueness in a larger scope.

879 8.2.6 Key path

880 When traversing a tree of objects from a given root object, the consecutive list of individual
881 local keys can be concatenated to what is referred to as a key path. From the perspective of a
882 given root object in an object tree a key path allows to uniquely identify any particular *Property*
883 and thereby its value.