

**OCPP 2.0.1**

Part 2 - Specification

FINAL, 2020-03-31

## Table of Contents

[Disclaimer 1](#_TOC_250016)

[Generic 2](#_TOC_250015)

[Version History 3](#_TOC_250014)

1. [Scope 4](#_TOC_250013)

[1.1. OCPP 2.0.1 4](#_TOC_250012)

1. [Conventions, Terminology and Abbreviations 5](#_TOC_250011)
   1. [Conventions 5](#_TOC_250010)
   2. [Terminology 6](#_TOC_250009)
   3. [Abbreviations 8](#_TOC_250008)
   4. [Actors 10](#_TOC_250007)
   5. [References 10](#_TOC_250006)
   6. [Definition of Transaction 12](#_TOC_250005)
   7. [ISO 15118 support 13](#_TOC_250004)
2. [Generic Requirements 15](#_TOC_250003)
   1. [Time Format Requirements 15](#_TOC_250002)
   2. [Message Timeouts 16](#_TOC_250001)
   3. [Language support 16](#_TOC_250000)
3. Security 17
   1. OCPP Security 18
      1. Security Objectives 18
      2. Design Considerations 18
      3. Security Profiles 19
      4. Keys used in OCPP 26
      5. Certificate Revocation 28
      6. Installation 28
   2. Use cases & Requirements 30

A01 - Update Charging Station Password for HTTP Basic Authentication 30

A02 - Update Charging Station Certificate by request of CSMS 31

A03 - Update Charging Station Certificate initiated by the Charging Station 34

A04 - Security Event Notification 38

A05 - Upgrade Charging Station Security Profile 39

1. Provisioning 41
   1. Introduction 42
      1. Transactions before being accepted by a CSMS 42
   2. Use cases & Requirements 43
      1. Booting a Charging Station 43

B01 - Cold Boot Charging Station 43

B02 - Cold Boot Charging Station - Pending 46

B03 - Cold Boot Charging Station - Rejected 49

B04 - Offline Behavior Idle Charging Station 51

* + 1. Configuring a Charging Station 52

B05 - Set Variables 52

B06 - Get Variables 54

B07 - Get Base Report 56

B08 - Get Custom Report 58

B09 - Setting a new NetworkConnectionProfile 60

B10 - Migrate to new CSMS 61

* + 1. Resetting a Charging Station 62

B11 - Reset - Without Ongoing Transaction 62

B12 - Reset - With Ongoing Transaction 65

1. Authorization 68
   1. Introduction 69
      1. ID Tokens 69
      2. Group ID Tokens 69
      3. Authorization Cache 70
      4. Local Authorization List 70
      5. Unknown Offline Authorization 70
   2. Use cases & Requirements 72
      1. Authorization options 72

C01 - EV Driver Authorization using RFID 72

C02 - Authorization using a start button 76

C03 - Authorization using credit/debit card 78

C04 - Authorization using PIN-code 81

C05 - Authorization for CSMS initiated transactions 83

C06 - Authorization using local id type 85

* + 1. ISO 15118 Authorization 88

C07 - Authorization using Contract Certificates 88

C08 - Authorization at EVSE using ISO 15118 External Identification Means (EIM) 91

* + 1. GroupId 93

C09 - Authorization by GroupId 93

* + 1. Authorization Cache 95

C10 - Store Authorization Data in the Authorization Cache 95

C11 - Clear Authorization Data in Authorization Cache 97

C12 - Start Transaction - Cached Id 98

* + 1. Local Authorization list 100

C13 - Offline Authorization through Local Authorization List 100

C14 - Online Authorization through Local Authorization List 101

* + 1. Offline Authorization 103

C15 - Offline Authorization of unknown Id 103

* + 1. Master Pass 105

C16 - Stop Transaction with a Master Pass 105

1. LocalAuthorizationList Management 108
   1. Introduction 109
   2. Use cases & Requirements 110

D01 - Send Local Authorization List 110

D02 - Get Local List Version 113

1. Transactions 114
   1. Introduction 115
      1. Flexible transaction start/stop 115
      2. TransactionId generation 115
      3. Delivering transaction-related messages 116
      4. Authorization 116
   2. Use cases & Requirements 117
      1. OCPP transaction mechanism 117

E01 - Start Transaction options 117

E02 - Start Transaction - Cable Plugin First 123

E03 - Start Transaction - IdToken First 128

E04 - Transaction started while Charging Station is offline 131

E05 - Start Transaction - Id not Accepted 135

E06 - Stop Transaction options 138

E07 - Transaction locally stopped by IdToken 143

E08 - Transaction stopped while Charging Station is offline 147

E09 - When cable disconnected on EV-side: Stop Transaction 150

E10 - When cable disconnected on EV-side: Suspend Transaction 153

E11 - Connection Loss During Transaction 156

E12 - Inform CSMS of an Offline Occurred Transaction 158

E13 - Transaction-related message not accepted by CSMS 160

E14 - Check transaction status 162

* + 1. Interrupting and Stopping ISO 15118 Charging 163

E15 - End of charging process 163

1. RemoteControl 165
   1. Introduction 166
   2. Use cases & Requirements 167
      1. Remote Transaction Control 167

F01 - Remote Start Transaction - Cable Plugin First 167

F02 - Remote Start Transaction - Remote Start First 170

F03 - Remote Stop Transaction 172

F04 - Remote Stop ISO 15118 Charging from CSMS 174

* + 1. Unlock Connector 177

F05 - Remotely Unlock Connector 177

* + 1. Remote Trigger 179

F06 - Trigger Message 179

1. Availability 182
   1. Introduction 183
   2. Use cases & Requirements 184

G01 - Status Notification 184

G02 - Heartbeat 185

G03 - Change Availability EVSE/Connector 187

G04 - Change Availability Charging Station 189

G05 - Lock Failure 191

1. Reservation 193
   1. Introduction 194
   2. Use cases & Requirements 195

H01 - Reservation 195

H02 - Cancel Reservation 199

H03 - Use a reserved EVSE 200

H04 - Reservation Ended, not used 203

1. TariffAndCost 204
   1. Introduction 205
      1. Why no structured tariff information? 205
   2. Use cases & Requirements 206

I01 - Show EV Driver-specific Tariff Information 206

I02 - Show EV Driver Running Total Cost During Charging 207

I03 - Show EV Driver Final Total Cost After Charging 208

I04 - Show Fallback Tariff Information 209

I05 - Show Fallback Total Cost Message 210

I06 - Update Tariff Information During Transaction 211

1. MeterValues 213
   1. Introduction 214
   2. Configuration 215
      1. Transaction Meter Values 215
      2. Clock-Aligned Meter Values 215
      3. Multiple Locations/Phases 216
      4. Signed Meter Values 216
   3. Use cases & Requirements 217
      1. MeterValues 217

J01 - Sending Meter Values not related to a transaction 217

J02 - Sending transaction related Meter Values 219

* + 1. ISO 15118 MeterValue signing 221

J03 - Charging Loop with metering information exchange 221

1. SmartCharging 223
   1. Introduction 224
   2. Types of Smart Charging 225
      1. Internal Load Balancing 225
      2. Central Smart Charging 225
      3. Local Smart Charging 225
      4. External Smart Charging Control Signals 226
   3. Charging profiles 228
      1. Introduction 228
      2. Charging profile purposes 228
      3. Charging profile recurrency 228
      4. Stacking charging profiles 229
      5. Combining Charging Profile Purposes 229
      6. Example Charging Profile 230
   4. Smart Charging Signals to a Charging Station from Multiple Actors 232
   5. Use cases & Requirements 233
      1. General Smart Charging 233

K01 - SetChargingProfile 233

K02 - Central Smart Charging 236

K03 - Local Smart Charging 239

K04 - Internal Load Balancing 242

K05 - Remote Start Transaction with Charging Profile 243

K06 - Offline Behavior Smart Charging During Transaction 245

K07 - Offline Behavior Smart Charging at Start of Transaction 246

K08 - Get Composite Schedule 248

K09 - Get Charging Profiles 250

K10 - Clear Charging Profile 251

* + 1. External Charging Limit based Smart Charging 252

K11 - Set / Update External Charging Limit With Ongoing Transaction 252

K12 - Set / Update External Charging Limit Without Ongoing Transaction 254

K13 - Reset / Release External Charging Limit 255

K14 - External Charging Limit with Local Controller 257

* + 1. ISO 15118 based Smart Charging 259

K15 - Charging with load leveling based on High Level Communication 259

K16 - Renegotiation initiated by CSMS 262

K17 - Renegotiation initiated by EV 264

1. FirmwareManagement 268
   1. Introduction 269
   2. Use cases & Requirements 270

L01 - Secure Firmware Update 270

L02 - Non-Secure Firmware Update 275

L03 - Publish Firmware file on Local Controller 279

L04 - Unpublish Firmware file on Local Controller 281

1. ISO 15118 CertificateManagement 283
   1. Introduction 284
   2. ISO 15118 Certificates 287
      1. ISO 15118 Certificate structure 287
      2. Using ISO 15118 Certificates in OCPP 288
      3. 15118 communication set-up 289
      4. Certificate - Use Case mapping 289
   3. Use cases from ISO 15118 relevant for OCPP 291
   4. Use cases & Requirements 292

M01 - Certificate installation EV 292

M02 - Certificate Update EV 293

M03 - Retrieve list of available certificates from a Charging Station 294

M04 - Delete a specific certificate from a Charging Station 295

M05 - Install CA certificate in a Charging Station 296

M06 - Get V2G Charging Station Certificate status 298

1. Diagnostics 300
   1. Introduction 301
   2. Use cases & Requirements 302
      1. Logging 302

N01 - Retrieve Log Information 302

* + 1. Configure Monitoring 304

N02 - Get Monitoring report 304

N03 - Set Monitoring Base 305

N04 - Set Variable Monitoring 306

N05 - Set Monitoring Level 309

N06 - Clear / Remove Monitoring 309

* + 1. Monitoring Events 310

N07 - Alert Event 310

N08 - Periodic Event 313

* + 1. Customer Information 315

N09 - Get Customer Information 315

N10 - Clear Customer Information 316

1. DisplayMessage 319
   1. Introduction 320
   2. Use cases & Requirements 321

O01 - Set DisplayMessage 321

O02 - Set DisplayMessage for Transaction 323

O03 - Get All DisplayMessages 325

O04 - Get Specific DisplayMessages 327

O05 - Clear a DisplayMessage 329

O06 - Replace DisplayMessage 330

1. DataTransfer 331
   1. Introduction 332
   2. Use cases & Requirements 333

P01 - Data Transfer to the Charging Station 333

P02 - Data Transfer to the CSMS 335

Messages, Datatypes & Enumerations 337

1. Messages 338
   1. Authorize 338
   2. BootNotification 338
   3. CancelReservation 339
   4. CertificateSigned 339
   5. ChangeAvailability 340
   6. ClearCache 340
   7. ClearChargingProfile 341
   8. ClearDisplayMessage 341
   9. ClearedChargingLimit 341
   10. ClearVariableMonitoring 342
   11. CostUpdated 342
   12. CustomerInformation 343
   13. DataTransfer 343
   14. DeleteCertificate 344
   15. FirmwareStatusNotification 344
   16. Get15118EVCertificate 345
   17. GetBaseReport 345
   18. GetCertificateStatus 346
   19. GetChargingProfiles 346
   20. GetCompositeSchedule 347
   21. GetDisplayMessages 347
   22. GetInstalledCertificateIds 348
   23. GetLocalListVersion 348
   24. GetLog 348
   25. GetMonitoringReport 349
   26. GetReport 350
   27. GetTransactionStatus 350
   28. GetVariables 351
   29. Heartbeat 351
   30. InstallCertificate 351
   31. LogStatusNotification 352
   32. MeterValues 352
   33. NotifyChargingLimit 352
   34. NotifyCustomerInformation 353
   35. NotifyDisplayMessages 353
   36. NotifyEVChargingNeeds 354
   37. NotifyEVChargingSchedule 354
   38. NotifyEvent 355
   39. NotifyMonitoringReport 355
   40. NotifyReport 356
   41. PublishFirmware 356
   42. PublishFirmwareStatusNotification 357
   43. ReportChargingProfiles 357
   44. RequestStartTransaction 358
   45. RequestStopTransaction 358
   46. ReservationStatusUpdate 359
   47. ReserveNow 359
   48. Reset 360
   49. SecurityEventNotification 360
   50. SendLocalList 360
   51. SetChargingProfile 361
   52. SetDisplayMessage 362
   53. SetMonitoringBase 362
   54. SetMonitoringLevel 362
   55. SetNetworkProfile 363
   56. SetVariableMonitoring 364
   57. SetVariables 364
   58. SignCertificate 365
   59. StatusNotification 365
   60. TransactionEvent 366
   61. TriggerMessage 367
   62. UnlockConnector 367
   63. UnpublishFirmware 368
   64. UpdateFirmware 368
2. Datatypes 370
   1. ACChargingParametersType 370
   2. AdditionalInfoType 370
   3. APNType 370
   4. AuthorizationData 371
   5. CertificateHashDataChainType 371
   6. CertificateHashDataType 371
   7. ChargingLimitType 371
   8. ChargingNeedsType 372
   9. ChargingProfileCriterionType 372
   10. ChargingProfileType 372
   11. ChargingSchedulePeriodType 373
   12. ChargingScheduleType 373
   13. ChargingStationType 374
   14. ClearChargingProfileType 374
   15. ClearMonitoringResultType 375
   16. ComponentType 375
   17. ComponentVariableType 375
   18. CompositeScheduleType 375
   19. ConsumptionCostType 376
   20. CostType 376
   21. DCChargingParametersType 376
   22. EventDataType 377
   23. EVSEType 377
   24. FirmwareType 378
   25. GetVariableDataType 378
   26. GetVariableResultType 378
   27. IdTokenInfoType 379
   28. IdTokenType 379
   29. LogParametersType 380
   30. MessageContentType 380
   31. MessageInfoType 380
   32. MeterValueType 381
   33. ModemType 381
   34. MonitoringDataType 381
   35. NetworkConnectionProfileType 381
   36. OCSPRequestDataType 382
   37. RelativeTimeIntervalType 382
   38. ReportDataType 382
   39. SalesTariffEntryType 383
   40. SalesTariffType 383
   41. SampledValueType 383
   42. SetMonitoringDataType 384
   43. SetMonitoringResultType 385
   44. SetVariableDataType 386
   45. SetVariableResultType 387
   46. SignedMeterValueType 387
   47. StatusInfoType 387
   48. TransactionType 388
   49. UnitOfMeasureType 388
   50. VariableAttributeType 388
   51. VariableCharacteristicsType 389
   52. VariableMonitoringType 389
   53. VariableType 390
   54. VPNType 391
3. Enumerations 392
   1. APNAuthenticationEnumType 392
   2. AttributeEnumType 392
   3. AuthorizationStatusEnumType 392
   4. AuthorizeCertificateStatusEnumType 392
   5. BootReasonEnumType 393
   6. CancelReservationStatusEnumType 393
   7. CertificateActionEnumType 393
   8. CertificateSignedStatusEnumType 394
   9. CertificateSigningUseEnumType 394
   10. ChangeAvailabilityStatusEnumType 394
   11. ChargingLimitSourceEnumType 394
   12. ChargingProfileKindEnumType 395
   13. ChargingProfilePurposeEnumType 395
   14. ChargingProfileStatusEnumType 395
   15. ChargingRateUnitEnumType 395
   16. ChargingStateEnumType 396
   17. ClearCacheStatusEnumType 396
   18. ClearChargingProfileStatusEnumType 396
   19. ClearMessageStatusEnumType 396
   20. ClearMonitoringStatusEnumType 397
   21. ComponentCriterionEnumType 397
   22. ConnectorEnumType 397
   23. ConnectorStatusEnumType 398
   24. CostKindEnumType 398
   25. CustomerInformationStatusEnumType 398
   26. DataEnumType 399
   27. DataTransferStatusEnumType 399
   28. DeleteCertificateStatusEnumType 399
   29. DisplayMessageStatusEnumType 399
   30. EnergyTransferModeEnumType 400
   31. EventNotificationEnumType 400
   32. EventTriggerEnumType 400
   33. FirmwareStatusEnumType 401
   34. GenericDeviceModelStatusEnumType 401
   35. GenericStatusEnumType 401
   36. GetCertificateIdUseEnumType 402
   37. GetCertificateStatusEnumType 402
   38. GetChargingProfileStatusEnumType 402
   39. GetDisplayMessagesStatusEnumType 402
   40. GetInstalledCertificateStatusEnumType 402
   41. GetVariableStatusEnumType 403
   42. HashAlgorithmEnumType 403
   43. IdTokenEnumType 403
   44. InstallCertificateStatusEnumType 403
   45. InstallCertificateUseEnumType 404
   46. Iso15118EVCertificateStatusEnumType 404
   47. LocationEnumType 404
   48. LogEnumType 404
   49. LogStatusEnumType 405
   50. MeasurandEnumType 405
   51. MessageFormatEnumType 406
   52. MessagePriorityEnumType 406
   53. MessageStateEnumType 407
   54. MessageTriggerEnumType 407
   55. MonitorEnumType 407
   56. MonitoringBaseEnumType 408
   57. MonitoringCriterionEnumType 408
   58. MutabilityEnumType 408
   59. NotifyEVChargingNeedsStatusEnumType 408
   60. OCPPInterfaceEnumType 409
   61. OCPPTransportEnumType 409
   62. OCPPVersionEnumType 409
   63. OperationalStatusEnumType 409
   64. PhaseEnumType 410
   65. PublishFirmwareStatusEnumType 410
   66. ReadingContextEnumType 410
   67. ReasonEnumType 411
   68. RecurrencyKindEnumType 411
   69. RegistrationStatusEnumType 411
   70. ReportBaseEnumType 412
   71. RequestStartStopStatusEnumType 412
   72. ReservationUpdateStatusEnumType 412
   73. ReserveNowStatusEnumType 413
   74. ResetEnumType 413
   75. ResetStatusEnumType 413
   76. SendLocalListStatusEnumType 413
   77. SetMonitoringStatusEnumType 414
   78. SetNetworkProfileStatusEnumType 414
   79. SetVariableStatusEnumType 414
   80. TransactionEventEnumType 414
   81. TriggerMessageStatusEnumType 415
   82. TriggerReasonEnumType 415
   83. UnlockStatusEnumType 416
   84. UnpublishFirmwareStatusEnumType 416
   85. UpdateEnumType 416
   86. UpdateFirmwareStatusEnumType 416
   87. UploadLogStatusEnumType 417
   88. VPNEnumType 417

Referenced Components and Variables 418

1. Controller Components 419
2. Referenced Components and Variables 420
   1. General 420
   2. Security related 427
   3. Authorization related 429
   4. Authorization Cache related 430
   5. Local Authorization List Management related 432
   6. Transaction related 433
   7. Metering related 435
   8. Reservation related 439
   9. Smart Charging related 440
   10. Tariff & Cost related 442
   11. Diagnostics related 444
   12. Display Message related 445
   13. Charging Infrastructure related 446
   14. ISO 15118 Related 449

## Disclaimer

Copyright © 2010 – 2020 Open Charge Alliance. All rights reserved.

This document is made available under the *\*Creative Commons Attribution-NoDerivatives 4.0 International Public License\**

(<https://creativecommons.org/licenses/by-nd/4.0/legalcode>).

# Generic

## Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description** |
| 2.0.1 | 2020-03-31 | Franc Buve (*OCA*) Milan Jansen (*OCA*) Paul Klapwijk (*OCA*)  Robert de Leeuw (*ihomer*) | Final version of OCPP 2.0.1 |
| 2.0 | 2018-04-11 | Anders Darander (*ChargeStorm*) Ben van Gameren (*IHomer*) Brendan McMahon (*ESB ecars*) Franc Buve (*OCA*)  Jonel Timbergen (*Alliander*) Klaas van Zuuren (*ElaadNL*) Milan Jansen (*OCA*)  Paul Klapwijk (*OCA*) Robert de Leeuw (*IHomer*)  Reinier Lamers (*New Motion*)  Robben Riksen (*Alliander*) | OCPP 2.0 April 2018  First major release since 1.0.  Lots of new/improved/revised functionality Revised documentation |
| 1.6 edition 2 | 2017-09-28 | Robert de Leeuw (*IHomer*) Brendan McMahon (*ESB ecars*) Klaas van Zuuren (*ElaadNL*) | OCPP 1.6 edition 2 Final release.  Contains all of the known erratas (including v3.0) and improved styling. |
| 1.6 | 2015-10-08 | Robert de Leeuw (*IHomer*) Reinier Lamers (*The New Motion*) Brendan McMahon (*ESB ecars*) Lambert Muhlenberg (*Alfen*) Patrick Rademakers (*IHomer*) Sergiu Tcaciuc (*smartlab*)  Klaas van Zuuren (*ElaadNL*) | 1.6 Final Release. |
| 1.5 | 2012-06-01 | Franc Buve |  |
| 1.2 | 2011-02-21 | Franc Buve |  |
| 1.0 | 2010-10-19 | Franc Buve | Final version approved by e-laad.nl. |

## Scope

This document defines the protocol used between a **Charging Station** and a **Charging Station Management System** in an EV charging infrastructure in the form of use cases. If the protocol requires a certain action or response from one side or the other, then this will be stated in this document.

This part of the specification does not define the communication technology. In order to ensure widespread compatibility OCPP

2.0.1 is limited to JSON. The specifications for the JSON implementation are in "Part 4 - JSON over WebSockets implementation guide".

### 1.1. OCPP 2.0.1

This specification defines version 2.0.1 of OCPP.

After the release of OCPP 2.0, some issues were found in OCPP 2.0. Some of these issues could not be fixed issuing errata to the specification text only, as has been done with OCPP 1.6, but required changes to the protocol’s machine-readable schema definition files that cannot be backward compatible.

To prevent confusion in the market and possible interoperability issues in the field, OCA has decided to name this version: 2.0.1. OCPP 2.0.1 contains fixes for all the known issues, to date, not only the fixes to the messages.

This version replaces OCPP 2.0. OCA advises implementers of OCPP to no longer implement OCPP 2.0 and only use version 2.0.1 going forward.

As a rule, existing numbered requirements are only updated or removed, previously used requirements numbers are never reused for a totally different requirement.

Any mentions of "OCPP 2.0" refers to revision 2.0.1 unless specifically stated otherwise.

## Conventions, Terminology and Abbreviations

### Conventions

#### Normative

All sections and appendices are normative, unless they are explicitly indicated to be informative.

#### Requirement Keywords

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and

"OPTIONAL" in this document are to be interpreted as described in RFC-2119 [RFC2119], subject to the following additional clarification clause:

The phrase "valid reasons in particular circumstances" relating to the usage of the terms "SHOULD", "SHOULD NOT", "RECOMMENDED", and "NOT RECOMMENDED" is to be taken to mean technically valid reasons, such as the absence of necessary hardware to support a function from a Charging Station design: for the purposes of this specification it specifically excludes decisions made on commercial, or other non-technical grounds, such as cost of implementation, or likelihood of use.

#### Primitive Datatypes

The specification mentions the following primitive datatypes:

*Table 1. Primitive Datatypes*

|  |  |
| --- | --- |
| **Datatype** | **Description** |
| string | The characters defined in the UTF-8 character set are allowed to be used. |
| integer | 32 bit (31 bit resolution, 1 sign bit) No leading 0’s  No plus sign  Allowed value examples: 1234, -1234  Not Allowed: 01234, +1234 |
| decimal | For data being reported by the Charging Station, the full resolution of the source data must be preserved. The decimal sent towards the Charging Station SHALL NOT have more than six decimal places. |
| identifierString | This is a case-insensitive dataType and can only contain characters from the following character set: a-z, A-Z, 0-9, '\*', '-', '\_', '=', ':', '+', '|', '@', '.' |
| dateTime | All time values exchanged between CSMS and Charging Station SHALL be formatted as defined in [RFC3339]. Additionally fractional seconds have been given an extra limit. The  number of decimal places SHALL NOT exceed the maximum of 3.  Example 1: 2019-04-12T23:20:50.52Z represents 20 minutes and 50.52 seconds after the 23rd  hour of April 12th, 2019 in UTC.  Example 2: 2019-12-19T16:39:57+01:00 represents 39 minutes and 57 seconds after the 16th hour of December 19th, 2019 with an offset of +01:00 from UTC (Central European Time). |
| AnyType | Text, data without specified length or format. |
| boolean | Only allowed values: "false" and "true". |

#### Normal communication

Unless otherwise specified, all use cases and requirements assume normal communication between Charging Station and CSMS (*Online*).

#### Field description

In many cases, further explanation about how or when to use certain fields in messages and datatypes is given in the field description. See Chapter Messages.

### Terminology

#### General Terminology

This section contains the terminology that is used throughout this document.

*Table 2. Terminology*

|  |  |
| --- | --- |
| **Terminology** | **Description** |
| **Application layer** | OSI-Layer 5-7. |
| **Authentication** | Authentication is the process of confirming an identity or attribute. When speaking about authentication one should distinguish between user authentication (e.g. sender/receiver) and message authentication. |
| **Block cipher** | Cryptographic primitive to encrypt/decrypt messages of fixed block length. Example: AES encrypts blocks of 128 bits (16 bytes) at a time. |
| **Cable Plugged in** | In this document this can mean the following:   * Cable fixed on Charging Station side, cable plugged in to EV * Cable plugged into the Charging Station and EV * Wireless Charger detects an EV |
| **Certificate** | A digital certificate authenticates a public key or entity. See also Public-Key Infrastructure. |
| **Certificate Management Protocol** | An internet protocol used to manage X.509 digital certificates within a PKI. It is described in RFC 4210 and uses the certificate request message format (CRMF) described in RFC 4211. |
| **Charging Cable** | Cable assembly equipped with a, by the EV accepted, plug, intended to be used for the connection between an EV and an EVSE. One side may be permanently attached to the EVSE, or also be equipped with a plug that is accepted by the EVSE. |
| **Charging Loop** | In this specification the ISO 15118-2 definition of the charging loop is used: *the V2G messaging phase for controlling the charging process by ISO 15118*. |
| **Charging Profile** | Generic Charging Profile, used for different types of Profiles. Contains information about the Profile and holds the ChargingSchedule. |
| **Charging Schedule** | Part of a Charging Profile. Defines a block of charging Power or Current limits. Can contain a start time and length. |
| **Charging Station** | The Charging Station is the physical system where EVs can be charged. A Charging Station has one or more EVSEs. |
| **Composite Charging Schedule** | The charging schedule as calculated by the Charging Station. It is the result of the calculation of all active schedules and possible local limits present in the Charging Station. Local Limits might be taken into account. |
| **Confidentiality** | Only authorized entities may access confidential data. To protect data from unauthorized access it can be encrypted. Then only entities with access to the secret keys can access the data after decrypting it. |
| **Connector** | The term Connector, as used in this specification, refers to an independently operated and managed electrical outlet on a Charging Station. In other words, this corresponds to a single physical Connector. In some cases an EVSE may have multiple physical socket types and/or tethered cable/Connector arrangements(i.e. Connectors) to facilitate different vehicle types (e.g. four-wheeled EVs and electric scooters). |
| **Contactor** | An electrically controlled switching device, typically used by Charging Stations to switch charging power on/off. |
| **Contract Certificate** | A valid certificate for a charging contract in an EV for 15118 communication. |
| **Control Pilot signal** | A signal used by a Charging Station to inform an EV of a maximum current limit, as defined by IEC61851-1. |
| **Cost** | Cost to be paid by an EV Driver for consumed energy/time etc. Including taxes. |
| **Cryptographic hash function** | Cryptographic hash functions should behave as one-way functions. They must be preimage resistant, 2nd preimage resistant, and collision-resistant. Changes in the input must produce explicitly different results in the output. Example: SHA-256. See also ENISA OCPP Security [1]. |
| **Cryptography** | The ENISA Algorithms, Key Sizes and Parameters Report [1] provides an overview of the current state of the art. |
| **CSMS** | Charging Station Management System. The system that manages Charging Stations and has the information for authorizing Users for using its Charging Stations. |
| **Data Integrity** | See Integrity and Message authentication. |

|  |  |
| --- | --- |
| **Terminology** | **Description** |
| **Digital Signature** | Authenticates the sender. In practice digital signatures are implemented using elliptic curves (EC). |
| **Encryption** | Using a cryptographic scheme, the message is mapped to a random-looking undecipherable string (ciphertext). Decryption reverses the encryption process and can only be performed with the corresponding decryption key. This decryption key is either the same as the encryption key (symmetric cryptography) or the private key in a public-key cryptosystem. The confidentiality of the message can be guaranteed only while the keys are kept secret. |
| **Energy Management System** | A device that manages the local loads (consumption an production) based on local and/or contractual constraints and/or contractual incentives. It has additional inputs, such as sensors and controls from e.g. PV, battery storage. |
| **Energy Offer Period** | Time during which a Charging Station is ready and willing to offer energy to an EV. |
| **Energy Transfer Period** | Time during which an EV chooses to take offered energy, or return it. |
| **EVSE** | An EVSE is considered as an independently operated and managed part of the Charging Station that can deliver energy to one EV at a time. |
| **Hash function** | Function that maps a message to a bit string of fixed length (hash value). See also cryptographic hash function. |
| **Hash value** | Output of a (cryptographic) hash function. The length is fixed in the specs of the hash function. |
| **High level communication** | bi-directional digital communication using protocol and messages and physical and data link layers specified in ISO 15118 series [ISO15118-1] |
| **Idle State** | In both use cases and sequence diagrams, *Idle* status is referred as the state in which a Charging Station is not performing any use case related tasks. Condition during which the equipment can promptly provide a primary function but is not doing so. |
| **Integrity** | Data cannot be altered without authorization. See also Message authentication. |
| **Local Controller** | A logical entity between a CSMS and one or more Charging Stations that has the ability to control charging of a group of Charging Stations based on the input from the CSMS, and can send messages to its Charging Stations, independently of the CSMS. |
| **Master Pass** | IdToken that can be used to stop any (or all) ongoing transactions. This can be used by for example law enforcement personal to stop a transaction. |
| **Master Pass UI** | Master Pass User Interface, this might be a full color touchscreen, but might also be just a couple of buttons and LEDs and/or sounds that enable a user to select transactions to be stopped. |
| **Message authentication** | Messages should be protected against unauthorized modifications. The message should always be sent together with an authentication tag providing its authenticity. Such an authentication tag can be the second output of an authenticated cipher such as AES-CCM or AES-GCM or a message authentication code. |
| **Mode of Operation** | A mode of operation specifies how the message blocks are processed by the block cipher. Using a block cipher in CBC or CTR mode provides encryption only, whereas using a block cipher in CCM or GCM mode encrypts the plaintext and produces a message authentication tag for the ciphertext. |
| **OCPP-J** | OCPP via JSON over WebSocket. |
| **Offline** | There is no communication possible between the Charging Station and CSMS. For an OCPP-J connection this means the WebSocket connection is not open. |
| **Password authentication** | The user proves his/her identity using a password or PIN. |
| **Phase Rotation** | Defines the wiring order of the phases between the electrical meter (or if absent, the grid connection), and the Charging Station Connector. |
| **Price** | Specific price tag of a single tariff entry, for example: 0.35 per kWh incl. 18% VAT. |
| **Public-key cryptography** | "Cryptographic scheme where a public key is published and henceforth can be used for encryption of messages or verification of digital signatures. Each public key has a counterpart, the corresponding private key. This key must be kept secret and is used for decryption or digital signing of messages. Public-key primitives have a high computational complexity for encryption and therefore are mostly used as part of a hybrid encryption scheme where the public key is used to communicate a common symmetric session key under which all further communication is encrypted. Certificates administered by a public-key infrastructure are used to establish the authenticity of the public key. See also ENISA OCPP Security [12]. The most popular public-key encryption scheme is RSA. Digital signatures can be generated most efficiently with elliptic-curve based (EC) mechanisms." |
| **Public-key infrastructure** | System to generate, administer, and revoke certificates. |
| **Resume regular transaction** | Used in sequence diagrams to indicate that this use case/sequence diagram has ended, but the transaction has not ended and will continue, but that is outside of scope of that specific use case. |

|  |  |
| --- | --- |
| **Terminology** | **Description** |
| **Requirement** | Provision that conveys criteria to be fulfilled. ISO/IEC Guide 2:2004, 7.5. |
| **Security Event** | Any event relevant to the secure operation of the device. |
| **Security Function** | Any function on the device that is needed for it to be operated securely, including access control, authentication, and encryption. |
| **Session** | A Session in OCPP is a general term that refers to the charging process of an EV, that might include a Transaction. |
| **Session key** | Symmetric key with a limited lifetime. |
| **Symmetric cryptography** | Sender and receiver hold the same key. Examples for symmetric primitives are block ciphers or MACs. |
| **Transaction** | A transaction in OCPP is a part of the complete process of charging an EV that starts and stops based on configurable parameters. These configurable parameters refer to moments in the charging process, such as the EV being connected or the EV driver being authorized. |
| **Tariff** | Collection of prices depending on charging time, power usage and other price affecting parameters. |
| **Use case** | A use case is a structured way of describing the (inter)actions necessary to achieve a certain objective. In this document, a use case consists of an actor list, a scenario description, postconditions and a sequence diagram and is always followed by a list of numbered requirements. |
| **User Authentication** | Verification of the identity of the communication partners (e.g., user on the device). Moreover, verification that the communication partners are still alive throughout a session. |

#### ISO 15118 and OCPP terminology mapping

*This section is informative.*

The ISO 15118 terminology is more comprehensive when referring to specific components within EVs and Charging Stations. The following table shows a "mapping" of these terms.

*Table 3. ISO 15118 and OCPP terminology mapping*

|  |  |
| --- | --- |
| **ISO 15118** | **OCPP** |
| ChargingProfile (contains the power over time the EV is planned to consume) | Loosely corresponds to ChargingSchedule in NotifyEVChargingSchedule message. |
| SASchedule (the power limits from a secondary actor for charging an EV for a specific time) | Loosely corresponds to ChargingProfile in SetChargingProfile message. |
| EVCC (i.e. Electric Vehicle Communication Controller) | Controller in the EV that is used for ISO 15118 communication. |
| Outlet | Connector |
| SECC (i.e. Supply Equipment Communication Controller) | Controller in the EVSE of the Charging Station that is used for ISO 15118 communication. |
| SA (i.e. Secondary Actor) | CSMS (or other backend systems) |

### Abbreviations

#### General Abbreviations

This section contains the abbreviations that are used throughout this document.

*Table 4. Abbreviations*

|  |  |
| --- | --- |
| **Abbreviation** | **Description** |
| **AES** | Advanced Encryption Standard. Original name for this block cipher was Rijndael named after its designers Vincent Rijmen and Joan Daemen. |
| **BEV** | Battery Electric Vehicle |
| **CMP** | Certificate Management Protocol |
| **CS** | Charging Station |
| **CSL** | Comma Separated List |
| **CSMS** | Charging Station Management System |

|  |  |
| --- | --- |
| **Abbreviation** | **Description** |
| **CSO** | Charging Station Operator |
| **DHCP** | Dynamic Host Configuration Protocol |
| **DNS** | Domain Name System |
| **DSO** | Distribution System Operator |
| **DST** | Daylight Saving Time |
| **EC** | Elliptic Curve. See also ENISA OCPP Security [1] |
| **ECDSA** | Elliptic Curve Digital Signature Algorithm. |
| **EMS** | Energy Management System |
| **ENISA** | European Union Agency for Network and Information Security. |
| **EV** | Electric Vehicle |
| **EVSE** | EV Supply Equipment IEC61851-1 |
| **FQDN** | Fully Qualified Domain Name |
| **FTP(S)** | File Transport Protocol (Secure) |
| **HTTP(S)** | HyperText Transport Protocol (Secure) |
| **ICCID** | Integrated Circuit Card Identifier |
| **IMSI** | International Mobile Subscription Identity |
| **JSON** | JavaScript Simple Object Notation |
| **MAC** | Message authentication code. Provides data integrity. Examples: CMAC, GMAC. See also ENISA OCPP Security [1]. |
| **NAT** | Network Address Translation |
| **NIST** | National Institute of Standards and Technology. |
| **NTP** | Network Time Protocol |
| **PDU** | Protocol Data Unit |
| **PHEV** | Plugin Hybrid Electric Vehicle |
| **RDN** | Relative Distinguished Name |
| **RSA** | Public-key cryptosystem named after its inventors Rivest, Shamir, and Adleman. |
| **RSA-PSS** | RSA-PSS is a new signature scheme that is based on the RSA cryptosystem and provides increased security assurance. It was added in version 2.1 of PKCS #1, following OCPP Security [23] |
| **RST** | 3 phase power connection, Standard Reference Phasing |
| **RTS** | 3 phase power connection, Reversed Reference Phasing |
| **SRT** | 3 phase power connection, Reversed 240 degree rotation |
| **STR** | 3 phase power connection, Standard 120 degree rotation |
| **TRS** | 3 phase power connection, Standard 240 degree rotation |
| **TSR** | 3 phase power connection, Reversed 120 degree rotation |
| **SC** | Smart Charging |
| **TLS** | Transport Layer Security |
| **TSO** | Transmission System Operator |
| **URI** | Uniform Resource Identifier RFC-3986 [RFC3986] |
| **URL** | Uniform Resource Locator - refers to the subset of URIs that, in addition to identifying a resource, provide a means of locating the resource by describing its primary access mechanism (e.g., its network "location"). |
| **UTC** | Coordinated Universal Time |
| **WAN** | Wide Area Network. |

#### ISO 15118 Abbreviations

This section contains the abbreviations from ISO 15118 that are used in this document.

*Table 5. ISO 15118 Abbreviations*

|  |  |
| --- | --- |
| **EIM** | External Identification Means |
| **EMAID** | E-Mobility Account Identifier |
| **EVCC** | EV Communication Controller |

|  |  |
| --- | --- |
| **HLC** | High Level Communication |
| **HMI** | Human Machine Interface |
| **LAN** | Local Area Network |
| **MO** | Mobility Operator |
| **OEM** | Original Equipment Manufacturer |
| **OCSP** | Online Certificate Status Protocol |
| **PWM** | Pulse Width Modulation |
| **SA** | Secondary Actor |
| **SECC** | Supply Equipment Communication Controller |
| **V2G** | Vehicle to Grid |

### Actors

*This section is informative.*

In OCPP, system actors are covering functions or devices.

*Table 6. Actors*

|  |  |  |
| --- | --- | --- |
| **Actor name** | **Actor type** | **Actor description** |
| EV Driver | Actor | The Driver of an EV who wants to charge the EV at a Charging Station. |
| Connector | Device | The term "Connector", as used in this specification, refers to an independently operated and managed electrical outlet on a Charging Station. In other words, this corresponds to a single physical Connector. In some cases an EVSE may have multiple Connectors: multiple physical socket types and/or types (e.g. four-wheeled EVs and electric scooters). |
| CSMS | System | Charging Station Management System: manages Charging Stations and has the information for authorizing Users for using its Charging Stations. |
| Charging Station | Device | The Charging Station is the physical system where an EV can be charged. A Charging Station has one or more EVSEs. |
| Charging Station Operator | Actor | A party that manages a CSMS. |
| Electric Vehicle | Device | Electric Vehicle, distributed energy resource with a remote battery and socket. |
| Local Controller | Device | A logical entity between a CSMS and one or more Charging Stations that has the ability to control charging of a group of Charging Stations based on the input from the CSMS. |
| External Control System | Actor | An external system that may impose charging limits/constraints on the Charging Station or CSMS, for example a DSO or EMS. |

### References

#### Generic references

*Table 7. References*

|  |  |
| --- | --- |
| **Reference** | **Description** |
| **[DNP3]** | Distributed Network Protocol. <https://www.dnp.org/About/Overview-of-DNP3-Protocol> |
| **[EMI3-BO]** | "eMI3 standard version V1.0" <http://emi3group.com/documents-links/> |
| **[IEC60870-5-104]** | Set of standards which define systems used for telecontrol (supervisory control and data acquisition) in electrical engineering and power system automation applications. <https://webstore.iec.ch/publication/3755> |
| **[IEC61850-7-420]** | Communications standard for distributed energy resources (DER). [https://webstore.iec.ch/](https://webstore.iec.ch/publication/6019) [publication/6019](https://webstore.iec.ch/publication/6019) |
| **[IEC61851-1]** | "IEC 61851-1 2017: EV conductive charging system - Part 1: General requirements" <https://webstore.iec.ch/publication/33644> |
| **[IEC62196]** | IEC 62196: Plugs, socket-outlets, vehicle couplers and vehicle inlets - Conductive charging of electric vehicles. <https://webstore.iec.ch/publication/6582> |

|  |  |
| --- | --- |
| **Reference** | **Description** |
| **[ISO15118-1]** | ISO 15118-1 specifies terms and definitions, general requirements and use cases as the basis for the other parts of ISO 15118. It provides a general overview and a common understanding of aspects influencing the charge process, payment and load leveling. [https://webstore.iec.ch/](https://webstore.iec.ch/publication/9272) [publication/9272](https://webstore.iec.ch/publication/9272) |
| **[ISO15118-2]** | Road vehicles – Vehicle to grid communication interface – Part 2: Technical protocol description and Open Systems Interconnection (OSI) layer requirements, Document Identifier: 69/216/CDV. <https://webstore.iec.ch/publication/9273> |
| **[ISO4217]** | "ISO 4217: Currency codes" <http://www.iso.org/iso/home/standards/currency_codes.htm> |
| **[OCPP2.0-PART4]** | "OCPP 2.0.1: Part 4 - JSON over WebSockets implementation guide". <http://www.openchargealliance.org/downloads/> |
| **[OpenADR]** | "Open Automated Demand Response" <http://www.openadr.org/> |
| **[RFC1321]** | "The MD5 Message-Digest Algorithm" <https://tools.ietf.org/html/rfc1321> |
| **[RFC2119]** | "Key words for use in RFCs to Indicate Requirement Levels". S. Bradner. March 1997. <http://www.ietf.org/rfc/rfc2119.txt> |
| **[RFC3339]** | "Date and Time on the Internet: Timestamps" <https://tools.ietf.org/html/rfc3339> |
| **[RFC3986]** | "Uniform Resource Identifier (URI): Generic Syntax" <https://tools.ietf.org/html/rfc3986> |
| **[RFC5646]** | "Tags for Identifying Languages" <https://tools.ietf.org/html/rfc5646> |

#### Security related references

*Table 8. Security related references*

|  |  |
| --- | --- |
| **Reference** | **Description** |
| **[1]** | ENISA European Network and Information Security Agency, Algorithms, key size and parameters report 2014, 2014. (last accessed on 17 January 2016) [https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-](https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014)  [report-2014](https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014) |
| **[2]** | National Institute of Standards and Technology. FIPS PUB 140-2, Security Requirements for Cryptographic Modules,  May 2001. <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf> |
| **[3]** | Cooper, D., et al., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,  Internet Engineering Task Force, Request for Comments 5280, May 2008, <http://www.ietf.org/rfc/rfc5280.txt> |
| **[4]** | Dierks, T. and Rescorla, E., The Transport Layer Security (TLS) Protocol Version 1.2, Internet Engineering Task Force,  Request for Comments 5246, August 2008, <http://www.ietf.org/rfc/rfc5246.txt> |
| **[5]** | Eastlake, D., Transport Layer Security (TLS) Extensions: Extension Definitions, Internet Engineering Task Force,  Request for Comments 6066, January 2011, <http://www.ietf.org/rfc/rfc6066.txt> |
| **[6]** | McGrew, D. and Bailey, D., AES-CCM Cipher Suites for Transport Layer Security (TLS), Internet Engineering Task Force,  Request for Comments 6655, July 2012, <http://www.ietf.org/rfc/rfc6655.txt> |
| **[7]** | Rescorla E. et al., Transport Layer Security (TLS) Renegotiation Indication Extension, Internet Engineering Task Force,  Request for Comments 5746, February 2010, <http://www.ietf.org/rfc/rfc5746.txt> |
| **[8]** | "Russel Housley, Tim Polk, Warwick Ford, and David Solo. Internet Public Key Infrastructure: X.509 Certificate and  Certificate Revocation List (CRL) Profile, RFC 3280, April 2002." <https://www.ietf.org/rfc/rfc3280.txt> |
| **[9]** | Pettersen. "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension." RFC 6961, June 2013.  <https://tools.ietf.org/html/rfc6961>. |
| **[10]** | Hollenbeck, S., "Transport Layer Security Protocol Compression Methods", RFC 3749, May 2004.  <https://www.ietf.org/rfc/rfc3749.txt> |
| **[11]** | National Institute of Standards and Technology. Annex C: Approved Random Number Generators for FIPS PUB 140-2  [25], February 2012. <https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexc.pdf> |
| **[12]** | Bundesamt für Sicherheit in der Informationstechnik: Anwendungshinweise und Interpretationen zum Schema, AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3.0, Bonn, Germany, May 2013. (in German) [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_pdf.html)  [Interpretationen/AIS\_20\_pdf.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_pdf.html) |
| **[13]** | Bundesamt für Sicherheit in der Informationstechnik: Anwendungshinweise und Interpretationen zum Schema, AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3.0, Bonn, Germany, May 2013. (in German) [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_pdf.html)  [Interpretationen/AIS\_31\_pdf.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_pdf.html) |

|  |  |
| --- | --- |
| **Reference** | **Description** |
| **[14]** | "OWASP - Transport Layer Protection Cheat Sheet. [https://www.owasp.org/index.php/](https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet#Extended_Validation_Certificates)  [Transport\_Layer\_Protection\_Cheat\_Sheet#Extended\_Validation\_Certificates](https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet#Extended_Validation_Certificates) " |
| **[15]** | P. Hoffman and W.C.A. Wijngaards, Elliptic Curve Digital Signature Algorithm (DSA) for DNNSEC, Internet Engineering  Task Force (IETF) RFC 6605, April 2012. <http://www.ietf.org/rfc/rfc6605.txt> |
| **[16]** | Adams, C., Farrell, S., Kause, T., and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management  Protocol (CMP)", RFC 4210, September 2005. <https://www.ietf.org/rfc/rfc4210.txt> |
| **[17]** | National Institute of Standards and Technology. Special Publication 800-57 Part 1 Rev. 4, Recommendation for Key  Management. January 2016. <https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/final> |
| **[18]** | RFC 2617. HTTP Authentication: Basic and Digest Access Authentication. <https://www.ietf.org/rfc/rfc2617.txt> |
| **[19]** | RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.  <https://www.ietf.org/rfc/rfc5280.txt> |
| **[20]** | OCPP 1.6. Interface description between Charging Station and CSMS. October 2015.  <http://www.openchargealliance.org/downloads/> |
| **[21]** | Eekelen, M. van, Poll, E., Hubbers, E., Vieira, B., Broek, F. van den: An end-to-end security design for smart EV-charging for Enexis and ElaadNL by LaQuSo1. December 2, 2014. [https://www.elaad.nl/smart-charging-end2end-security-](https://www.elaad.nl/smart-charging-end2end-security-design/)  [design/](https://www.elaad.nl/smart-charging-end2end-security-design/) |
| **[22]** | RFC 2986. PKCS #10: Certification Request Syntax Specification, Version 1.7. <https://www.ietf.org/rfc/rfc2986.txt> |
| **[23]** | RSA-PSS. <https://tools.ietf.org/html/rfc8017> |
| **[24]** | Santesson, et al. "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP" RFC 6960. June  2013. <https://tools.ietf.org/html/rfc6960> |
| **[25]** | RFC 2818. HTTP Over TLS. <https://tools.ietf.org/html/rfc2818> |

### Definition of Transaction

*This section is informative.*

To support as many business cases as possible, and to prevent too many messages being sent when not needed for certain business cases, OCPP 2.0.1 supports flexible configuration of the start and stop of a transaction. This makes it possible to define the start and stop of a transaction depending on market demands.

See: Flexible transaction start/stop for more information.

#### Transaction in relation to Energy Transfer Period

The Energy Transfer Period is a period of time during which energy is transferred between the EV and the EVSE. There MAY be multiple Energy Transfer Periods during a Transaction.

Multiple Energy Transfer Periods can be separated by either:

* + - * an EVSE-initiated suspense of transfer during which the EVSE does not offer energy transfer, *or*;
      * an EV-initiated suspense of transfer during which the EV remains electrically connected to the EVSE, *or*;
      * an EV-initiated suspense of transfer during which the EV is not electrically connected to the EVSE.

Transaction

Energy Offer

Energy Flow

###### Transaction



Transaction start is configured via configuration Variable: TxStartPoint

###### EnergyOfferPeriod

Energy Offer Period starts when the EVSE is ready and willing to supply energy.

###### EnergyTransferPeriod

Energy is transferred.

During an EnergyOfferPeriod there may be periods the EV is not charging due to for instance, warm/full battery or EV internal smart charging.

###### EnergyTransferPeriod

Energy is transferred.

###### EnergyOfferSuspendPeriod

During a transaction, there may be periods the EnergyOffer to EV is suspended by the EVSE, for instance due to Smart Charging or local balancing.

###### EnergyOfferPeriod

**EnergyTransferPeriod**

Energy is transferred.

Transaction stop is configured via configuration Variable:

TxStopPoint

*Figure 1. OCPP Charging Transaction definition*

### ISO 15118 support

*This section is informative.*

This version of OCPP supports ISO 15118 authorization (also called "Plug and Charge") and ISO 15118 based Smart Charging. (See [ISO15118-2]) Furthermore it describes how to install and update ISO 15118 certificates. These 3 functionalities are not included as

one functional block, but are included in multiple chapters throughout the specification. ISO 15118 authorization is included in the functional block Authorization and the Smart Charging use cases for ISO 15118 are included in the chapter Smart Charging.

Certificate handling is described in a separate functional block.

Implementors of 15118 need to be aware of timeout constraints enforced by 15118, see [ISO15118-1] (Page: 127, Table: 109) For reference, the current timing constrains for 15118 edition 1 are:

*Table 9. ISO 15118 Timing constrains*

|  |  |
| --- | --- |
| **Timeout** | **Default** |
| Sequence Timeouts | 60 seconds |
| Sequence Performance Timeouts | 40 seconds |
| PaymentDetailsReq/Res | 5 seconds |
| CertificateUpdateReq/Res | 5 seconds |
| CertificateInstallationReq/Res | 5 seconds |

## Generic Requirements

*This section is normative.*

The generic requirements build the basis for defining the use case elements described in the Functional Blocks.

*Table 10. Generic requirements*

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Precondition** | **Requirement definition** | **Note** |
| FR.01 |  | The sender of a <message>Request SHALL wait for a  <message>Response or a timeout, before sending another request message. |  |
| FR.02 | When the Charging Station receives a valid OCPP request message according to the JSON schemas / RPC  Framework AND  the other system is not causing a security violation | The Charging Station SHALL respond with a RPC Framework: CALLRESULT. | If the Charging Station/CSMS needs to provide additional information, this can be done in the *statusInfo* element of the response message. |
| FR.03 | When the Charging Station/CSMS receives an invalid OCPP message according to the JSON schemas / RPC  Framework OR  the other system causes a security violation | The Charging Station/CSMS SHALL respond with a RPC Framework: CALLERROR. |  |
| FR.04 | When the CSMS did not accept the BootNotificationRequest from the  Charging Station AND  The Charging Station sends a message other than BootNotificationRequest | The CSMS SHALL respond with a RPC Framework: CALLERROR: SecurityError. |  |

### Time Format Requirements

*This section is normative.*

All time values exchanged between CSMS and Charging Station SHALL be formatted as defined in RFC-3339 [RFC3339]. Additionally fractional seconds have been given an extra limit. The number of decimal places SHALL NOT exceed the maximum of

3. However, it is RECOMMENDED to omit fractional seconds entirely, because it is of limited use and omitting it reduces data usages.

It is strongly RECOMMENDED to exchange all time values between CSMS and Charging Station as UTC, with the time zone designator 'Z', as specified by RFC-3339 [RFC3339]. This will improve interoperability between CSMS and Charging Station.

#### Displaying local time

When a Charging Station wants to give detailed control of configuring the internal clock to a CSO, it can implement one or more of the following Configuration Variables: TimeSource, TimeZone, TimeOffset, NtpSource, NtpServerUri.

##### Daylight Saving Time

There are 2 ways a Charging Station can support punctual automated bi-annual changeover between "standard time" and "daylight saving time" periods.

* + - * + The transition dates and offsets are known in the Charging Station, based on the configured TimeZone.
        + The transition date and offset is manually configured for every transition via: NextTimeOffsetTransitionDateTime

and TimeOffsetNextTransition.

Daylight saving time is used for displaying the current time to the EV driver.

### Message Timeouts

*This section is normative.*

OCPP does not specify timing requirements for messages. Timing of messages is greatly influenced by the underlying network used. A GPRS network has different timing characteristics compared to a land-line. As OCPP does not require a certain type of network, but leaves this open for the CSO to select, OCPP cannot require timing constrains.

If you are looking for some guidance, start with a 30 second timeout on message requests, and tune it for the network used.

The message timeout setting in a Charging Station can be configured in the messageTimeout field in the NetworkConnectionProfile. The purpose of the message timeout is to be able to consider a request message as not sent and continue with other tasks when the message did not arrive due to communication errors or software failure. For transaction related events, use case E13 - Transaction-related message not accepted by CSMS describes the retry procedure when this happens. See also the section Delivering transaction-related messages in Functional Block E.

### Language support

*This section is informative.*

A CSMS can provide the Charging Station with preferred languages for an EV Driver, enabling the Charging Station to communicate with the EV Driver in a language according to his/her preferences.

For any Charging Station that shows messages on a display it is RECOMMENDED to at least also implement these in "English". When the preferred languages for an EV-driver (provided by the CSMS) are not "English" and don’t match any of the other languages implemented in the Charging Station, it is RECOMMENDED to use "English" as fall-back.