OCPP for Resource-Constrained Devices

Version 1, March 2025

Table of Contents

Management summary

This document addresses the challenges of implementing the Open Charge Point Protocol (OCPP) 2.0.1 on resource-constrained devices, such as microcontrollers used in lightweight electric vehicle charging stations. With limited RAM, ROM, and flash memory available, it is impractical to deploy the entire protocol. The focus is on achieving a minimal yet compliant implementation, prioritizing the "Core" profile of OCPP while omitting optional features that are not essential for basic functionality.

Key strategies include minimizing firmware size, reducing memory usage, and optimizing message handling. For example, read-only variables avoid the need for embedded databases, while smaller TLS buffer sizes help reduce memory demands. Real-world benchmarks from MicroOCPP demonstrate that a streamlined implementation can operate within 50 kB of RAM and 200 kB of ROM, making it viable for low-resource environments.

By tailoring OCPP to resource-limited devices, this approach ensures interoperability with existing systems while enabling cost-effective deployment of charging infrastructure. This balance between efficiency, scalability, and compliance is critical to supporting the growth of EV charging networks.

1. Introduction

The Open Charge Point Protocol (OCPP) is a communication protocol specifically designed for the exchange of information between electric vehicle (EV) charging stations and their management systems. It enables the authentication of EV drivers, manages charging sessions, and monitors the performance of charging stations.

Over the past 15 years, OCPP has evolved in tandem with the electric vehicle charging industry. Currently, the most widely adopted version of OCPP for resource-constrained devices is OCPP 1.6, which was published in 2015. This version encompasses essential functions for authorization and transaction handling, and it provides optional profiles for smart charging, security, and firmware management. Despite being a decade old, OCPP 1.6 remains actively supported by the Open Charge Alliance (OCA), which continues to manage errata, conduct testing events, and enhance the conformance testing tool and certification program. However, no new features are being added to OCPP 1.6; all new development efforts are focused on the OCPP 2.x series, which represents a significant advancement introduced in 2020.

Looking ahead, it is imperative that resource-constrained devices are able to benefit from the ongoing feature development in EV charging, implementing OCPP 2.x in a manner compatible with their hardware. For charging network operators, utilizing a single version of OCPP to manage their entire portfolio of charging stations—from fast chargers to basic wall boxes—will enhance operational efficiency. Furthermore, regulators can reference a single version of OCPP, thereby consolidating efforts and clarifying regulations. This paper will explore the implementation of OCPP 2.0.1 (or OCPP 2.x in general) in the most streamlined manner possible: OCPP 2.Lite.

The OCPP 2.0.1 specification comprises over 1,500 pages. In contrast, the OCPP 1.6 release is approximately 150 pages long, which might lead to the assumption that an OCPP 2.0.1 implementation would be ten times larger than that of OCPP 1.6. This is not necessarily accurate. This paper will demonstrate that a "light" OCPP 2.0.1 implementation, devoid of optional features, can be of comparable size or only marginally larger than OCPP 1.6.

Currently, two minimal implementations, that are based upon the recommendation in this paper, are under development: MicroOCPP [MicroOCPP] and OpenOCPP [OpenOCPP]. Preliminary results suggest that the OCPP protocol stack of these implementations, that support both OCPP 1.6 and 2.0.1, will fit within 200 KB. The size of a full firmware image for a charging station will vary with the capabilities and features or a charging station, but is expected to remain below 2 MB.

Once these implementations are ready and available as open source, their findings will be added as case studies in an updated version of this paper.

Flexibility for Certification Purposes: Profiles, Features, and Product Types

Globally, OCPP is utilized across a diverse range of charging stations, from basic to advanced models, and from low-power to high-power systems, including bidirectional charging stations. However, not all features outlined in the OCPP specification are universally required. As such, many features within OCPP are optional, enabling implementers to select functionalities that best align with their specific requirements while still ensuring interoperability with other OCPP implementations, provided that the core components have been implemented.

Some implementers choose to incorporate all features specified in OCPP 2.0.1. For example, providers of OCPP software stacks often deliver a comprehensive range of features to their clients. Similarly, Charging Station

Management System providers may choose to support a broad spectrum of charging station types across various regions. Conversely, many implementers may only necessitate a subset of the available features, depending on the type of charger being developed (e.g., for light electric vehicles) or the specific use cases to be supported (e.g., remote start functionality).

The OCPP specification includes mechanisms to accommodate the diverse needs of implementers:

1. **OCPP Profiles:** Part 5 of the OCPP specification delineates "Profiles," which define a set of supported functions. The "Core" profile encompasses fundamental OCPP functionalities such as security, authentication, charging session management, and charging station management. Additionally, there are seven other profiles that address advanced features, including advanced security, local list management, smart charging, enhanced user interfaces (e.g., displays), advanced device management, charging station reservation, and ISO 15118 support. The forthcoming OCPP 2.1 version will introduce two additional profiles: V2X (bidirectional power transfer) and DER control (utility management of distributed energy resources).
2. **OCPP Features within a Profile:** This includes both hardware-related and optional features:
    - **Hardware Features:** Specific hardware components of a charging station (e.g., fixed charging cables, credit card readers, or displays) may affect OCPP behavior and determine the applicability of certain OCPP functionalities.
    - **Optional Features:** Numerous behaviors detailed in the OCPP specification are optional. Implementers possess the flexibility to choose which features to support, such as various authentication methods (e.g., RFID, QR code, credit card reader), diverse transaction initiation points (e.g., upon connection of the charging cable or commencement of energy flow), or support for offline transactions.
3. **Product Types for Certification:** The required test suite for certification varies according to the OCPP Product Type:
    - Charging station management systems
    - Charging stations
    - Software stacks for a charging station
    - Mode 1/2-only charging stations (lacking communication with the EV)

These mechanisms provide the EV charging industry freedom to build their charging networks according to their needs, whilst still ensuring interoperability.

This paper investigates, considering resource-constrained devices, the characteristics of a minimum implementation of OCPP 2.0.1 and the resources necessary for its realization.

2. Resource-constrained devices

Public and residential AC charging stations often incorporate a microcontroller for the OCPP communication, for example the Espressif32 or STM32. These microcontrollers are designed for special-purpose systems such as in-field nodes in Internet-of-Things (IoT) networks, but they can also be used as the network controller in charging stations. This class of microcontrollers is constrained in terms of RAM and ROM capacity: usually limited to a few hundred kilobytes of RAM and a few megabytes of ROM.

The OCPP software that is running on a charging station has an impact on the following resources:

- CPU cycles: a series of steps that the CPU goes through to fetch, decode and execute instructions.
- RAM (random access memory): A running application will require working memory for a stack and heap to store data.
- ROM (read-only memory): The OCPP firmware itself is read-only memory.
- Flash memory: This is persistent memory, which is used, for example, to store configuration settings.

Data communication usage does not relate to resource limitations on the device, but we will address it in section Data communication and OCPP messages sizes.

As it turns out, CPU cycles are not a bottleneck as far as OCPP is concerned. OCPP is about transferring information between charging station and backend (CSMS). CPU cycles are mostly used for work related to TLS encryption/decryption and message parsing and not much else.

The most serious constraint will be memory. The firmware is stored in read-only memory (ROM); a smaller firmware image requires less ROM. A running application requires working memory for a stack and heap to store data. This is stored in random-access memory (RAM). The last type of memory is persistent memory, which is used, for example, to store configuration settings. Persistent memory in charging stations often is flash memory.

In this paper we will focus on:

- Minimizing ROM usage (directly related to size of firmware image)
- Minimizing RAM usage (working memory)
- Minimizing persistent memory usage
- Minimizing device model size (affecting both RAM and persistent memory)

In APPENDIX B: Case study MicroOCPP we provide a case study with real-world data of an example minimal implementation of the OCPP protocol stack optimized for the usage on microcontrollers. This data provides insights into how much memory is used for OCPP. It can be used as a basis for estimating the resource requirements of the OCPP interface and selecting microcontrollers according to the memory needs.

APPENDIX C: Case study OpenOCPP describes the ROM and RAM resource usage of a minimal implementation for a complete charging station firmware.

3. Minimizing ROM usage

There are two important factors that help to minimize ROM usage. One is to avoid using an embedded database for the device model. This option is discussed in Minimizing device model size. The other is to minimize the size of the firmware image by reducing the program logic and the associated number of messages that we implement.

The OCPP functionality has been grouped in a number of profiles that represent a set of related use cases. Any charging station needs to support at least the Core profile in order to be eligible for certification. All other profiles are optional. The certification profiles are defined in [OCPP-Part5] and summarized below in table

Certification profiles.

Table 1. Certification profiles

Certification Profile	Description
Core	Basic functionality of OCPP
Advanced Security	Advanced security with client certificates
Local Authorization List Management	Support for local white lists
Smart Charging	Support for smart charging with charging schedules
Advanced Device Management	Variable monitoring and custom reports
Advanced User Interface	Support for messages, tariff and cost on display
Reservation	Reservation of an EVSE
ISO 15118 support	Support for ISO 15118-2

In this section we describe the minimal set of use cases and messages that need to be supported for sections A to P of the specification in [OCPP-Part2]. The data is summarized in the table Minimum message set in APPENDIX A: Summary of messages per section.

Section A. Security

Security profile 3 is not part of the Core profile. The messages SignCertificate and CertificateSigned are only needed in the context of security profile 3 and can therefore be omitted.

Required messages:

- SetVariables
- SecurityEventNotification

Section B. Provisioning

In the OCPP 2.0.1 Core profile the only use case in B that is not mandatory is B08 Get Custom Report. This means that the GetReport message does not require implementing. There is no loss in functionality, since all device model information can be retrieved via the GetBaseReport message.

In addition, the messages GetVariables and SetVariables can have a slightly simpler implementation if the number of items per message is set to 1 via ItemsPerMessage[Set/GetVariables].

Required messages:

- BootNotification

- SetVariables
- GetVariables
- GetBaseReport
- NotifyReport
- SetNetworkProfile
- Reset

Section C. Authorization

In the OCPP 2.0.1 Core profile, several authorization methods are described, of which at least one must be implemented. A minimal implementation therefore only has to support a single authorization method. This is likely to be one of C01 (RFID) or C02 (start button), or it only supports remote authorization by CSMS, as described in C04. The use of a local authorization cache to reduce authorization time is optional in the Core profile and can be omitted, since this would require additional persistent storage.

Required messages, one or both of:

- Authorize (for C01 or C02), or
- RequestStartTransaction (for C04)

Section D. Local Authorization List

Section D of the OCPP 2.0.1 specification describes functionality to authorize a user via a local white list. This can be used when the charging station is offline, or to reduce authorization response time when the charging station is online. Storing a local authorization list requires additional persistent storage, and can be omitted for a ‘Lite’ implementation. Since Local List Management is a separate optional certification profile in OCPP 2.0.1 anyway, a ‘Lite’ implementation does not differ from a regular OCPP 2.0.1 Core implementation.

Section E. Transactions

To accommodate for the various business models arising in the EV charging industry, OCPP 2.0.1 added flexible start and stop points of a transaction. This does introduce complexity in the firmware though, because the behavior of certain use cases changes depending on when the transaction starts or ends. This complexity can be removed by fixing the start and stop points of the transaction. If both TxStartPoint and TxStopPoint are set to PowerPathClosed then a transaction is started when the user is authorized and the cable is connected, and the transaction stops when authorization ends or cable is disconnected.

This is the same behavior as in OCPP 1.6. The use cases E02 and E03 become equivalent. Use case E04 is not supported, because there is no authorization cache or local authorization list. (See Section C. Authorization and Section D. Local Authorization List.)

Use case E14 (GetTransactionStatus) is required for the "Core" profile of OCPP. It enables the CSMS to request the status of a transaction and to find out whether there are queued transaction-related messages — a situation that may occur when the charger has been offline for a while.

Required messages:

- TransactionEvent
- GetTransactionStatus

Section F. Remote control

Remote control is about remotely authorizing for a transaction and remotely stopping it, remotely unlocking a connector, and triggering a charging station to perform a certain action.

Remote start/stop and unlock connector are required, and may be the only method to start and stop a transaction if local authorization is not implemented. Support for TriggerMessage is optional.

Required messages:

- RequestStartTransaction
- RequestStopTransaction
- UnlockConnector (only in case of a detachable cable)

Section G. Availability

The notification of availability status and heartbeats is part of Core functionality and must be implemented.

Required messages:

- StatusNotification or NotifyEvent
- Heartbeat
- ChangeAvailability

Section H. Reservation

The functionality of Reservation may not be required for resource-constrained devices. Since ‘Reservations’ is a separate optional certification profile in OCPP 2.0.1 anyway, a ‘Lite’ implementation does not differ from a regular OCPP 2.0.1 implementation

Section I. Tariff and Cost

This Functional Block provides tariff and cost information to an EV Driver, if a Charging Station is capable of showing this on a display. It is assumed that resource-constrained devices either do not have a display or have a display that is not actively managed by the CSMS. Therefore, the Tariff and Cost functionality can be omitted. Since this is a separate optional certification profile in OCPP 2.0.1 anyway, a ‘Lite’ implementation does not differ from a regular OCPP 2.0.1 implementation.

Section J. Meter Values

Transaction-related meter values are sent via the TransactionEvent message. There is also a separate MeterValues message that can be used to send clock-aligned meter values outside of a transaction.

Required messages:

- TransactionEvent
- MeterValues

Section K. Smart Charging

Smart charging is not part of the OCPP "core" profile, but there might be a reason to include this in certain minimal implementations anyhow. Home chargers are likely candidates for minimal implementations, and certain in some countries they are required to support smart charging functionality.

A full implementation of smart charging with multiple charging profile kinds and stack levels may be too much for a minimal implementation, so certain limitations are needed in that case:

- The number of charging profiles that a charging station can hold is limited to 1 or 2. That suffices for a TxProfile and/or a TxDefaultProfile.
- The number of periods in a charging schedules is limited to, for example, 3 periods. (Most charging schedules do not have more than 3 periods, anyhow).
- Only a single stack level is supported.

The above reduces memory requirements and simplifies the implementation of a GetCompositeSchedule message.

Required messages (when supporting smart charging):

- SetChargingProfile
- ClearChargingProfile
- GetCompositeSchedule
- Get/ReportChargingProfiles

Section L. Firmware Management

A minimal implementation still needs to be able to update its firmware and do this in a secure manner. Use case L01 Secure Firmware Update is part of OCPP Core profile, and is therefore required in a minimal implementation.

Required messages:

- UpdateFirmware
- FirmwareStatusNotification

Section M. ISO 15118 Certificate Management

Support of ISO 15118 is not expected of a minimal implementation. Some functionality of certificate management, however, of this section is required to implement security profile 2, namely use case M05 InstallCertificate to install the CSMS root certificate.

Required messages:

- InstallCertificate
- GetInstalledCertificateIds
- DeleteCertificate

Section N. Diagnostics

The advanced diagnostic features are part of the optional certification profile ‘Advanced Device Management’. The functionality to download log files (N01 Retrieve Log Information) and to report customer information (N09/N10 Get/Clear Customer Information) are part of the OCPP 2.0.1 Core profile. The use cases N09 and N10 with messages CustomerInformation and NotifyCustomerInformation, however, have a limited use and are not required for normal operation. Functionality to report and clear customer information (N09/N10 Get/Clear Customer Information) was added to adhere to privacy regulation (e.g. GDPR in Europe). If a minimal implementation does not store any customer information, because it does not have the space for this, then implementation of these messages becomes very trivial.

Only use case N01 Retrieve Log Information is required.
Required messages:

- GetLog
- LogStatusNotification
- CustomerInformation
- NotifyCustomerInformation

Section O. Display Messages

This functional block enables an operator to remotely display a message or a cycle of messages on a charging station. It is assumed that resource-constrained devices either do not have a display or have a display that is not actively managed by the CSMS. Therefore, the Display Message functionality can be omitted. Since this is a separate optional certification profile in OCPP 2.0.1 anyway, a ‘Lite’ implementation does not differ from a regular OCPP 2.0.1 implementation

Section P. DataTransfer

This functional block describes functionality to send custom message via the DataTransfer message. DataTransfer messages need not be supported, but the minimal implementation must be able to reject them when received.

4. Minimizing RAM usage

This section provides three ways to reduce the required RAM usage: by limiting the sizes of certain message, by avoiding data duplication, and by reducing the size of the TLS buffer.

4.1. Limiting message sizes

RAM memory is used for stack and heap memory. It is used to store data that is processed, for example while decoding incoming messages or encoding messages to be sent. The amount of memory required to decode messages upon receipt or construct messages before sending can be limited by the following configuration variables:

- DeviceDataCtrlr.ItemsPerMessage
- DeviceDataCtrlr.BytesPerMessage
- DeviceDataCtrlr.ReportingValueSize
- MonitoringCtrlr.ItemsPerMessage
- MonitoringCtrlr.BytesPerMessage
- SmartChargingCtrlr.PeriodsPerSchedule
- SampledDataCtrlr.TxStarted/Updated/EndedMeasurands
- AlignedDataCtrlr.Measurands

These configuration variables limit the size of potentially very large messages.

4.2. Avoiding data duplication in RAM

Data transmission in an OCPP implementation takes several steps. For incoming messages, the data is first received on the networking interface, then the TLS library decrypts it, providing the data to a WebSocket client which buffers all data until a JSON message is complete. Depending on the architecture of the OCPP implementation, the JSON message could further be copied and forwarded to message listeners until it is finally consumed. It looks similar in the other direction. This multistep pipeline potentially means that a buffer between any two steps holds a full copy of the payload data sent via OCPP, which is a common pitfall of implementing OCPP.

There is a significant optimization potential in avoiding copying the unencrypted data in RAM. For incoming messages, that would mean keeping the JSON message in the TLS input buffer, instructing the JSON library to parse the JSON object in place and only copying data when updating the final data model. Of course, the exact approach of avoiding data duplication depends on the software architecture but should be similar to this description. For outgoing messages, the same idea should be considered.

It is important to pay special attention to the heap consumption behavior during receipt and sending of messages. Usually, the heap occupation spikes during message processing and for microcontrollers, the worst-case heap occupation is the most relevant aspect to optimize for.

4.3. Reducing TLS communication buffer

A TLS communication by default requires two 16 kB buffers. This buffer can be reduced by adapting the TLS fragment length.

TLS involves sending "Records" between peers. Records can be of type “Handshake”, “Alert”, “ChangeCipherSpec”, “Heartbeat” or “Application”. OCPP messages are sent in Application records. The payload contains a “fragment” of the application data. The record layer fragments information blocks into TLSPlaintext records carrying data in chunks of 2^14 bytes (16kB) or less.

TLS peers need to maintain an input and an output buffer to store an entire fragment of 16 kB. For a low resource device it is a large cost to allocate 32 kB for the TLS connection.

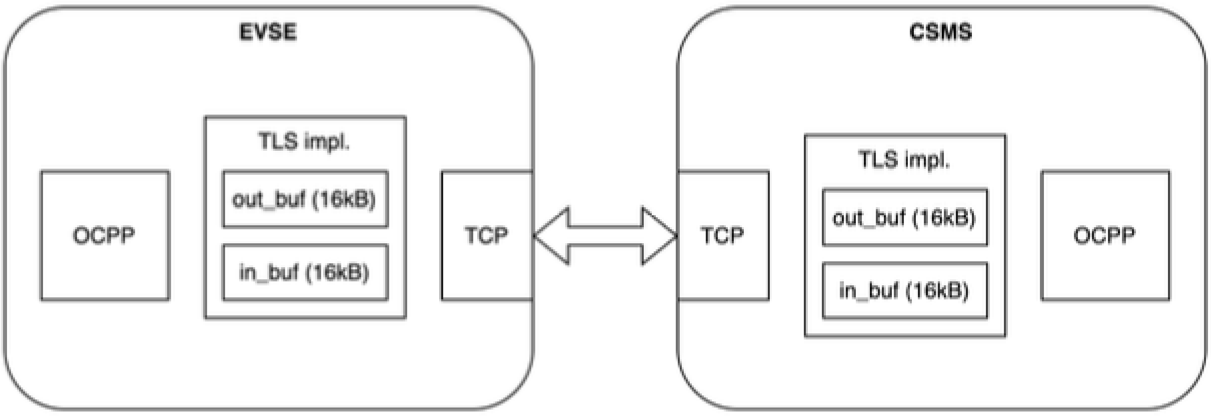

Figure 1. Peers allocating standard 16 kB TLS buffers

A TLS extension is defined in TLS Extensions RFC6066 Section 4, that allows the client to ask for a different maximum fragment length than the default 16kB. A client can ask for a maximum fragment length of 0.5 kB, 1 kB, 2 kB or 4 kB. This TLS extension is, however, not widely supported and native managed cloud TLS termination services typically don't support this.

A resource-constrained Charging Station SHOULD try to negotiate a smaller TLS maximum fragment size, and if that is not accepted by the peer, then Charging Station MAY unilaterally decide to allocate less memory to its TLS output buffer. A TLS maximum fragment length of 2 kB is suggested based on data collection during certification tests, which shows that 99% of the messages fit in a 2 kB buffer. This is described in the next section.

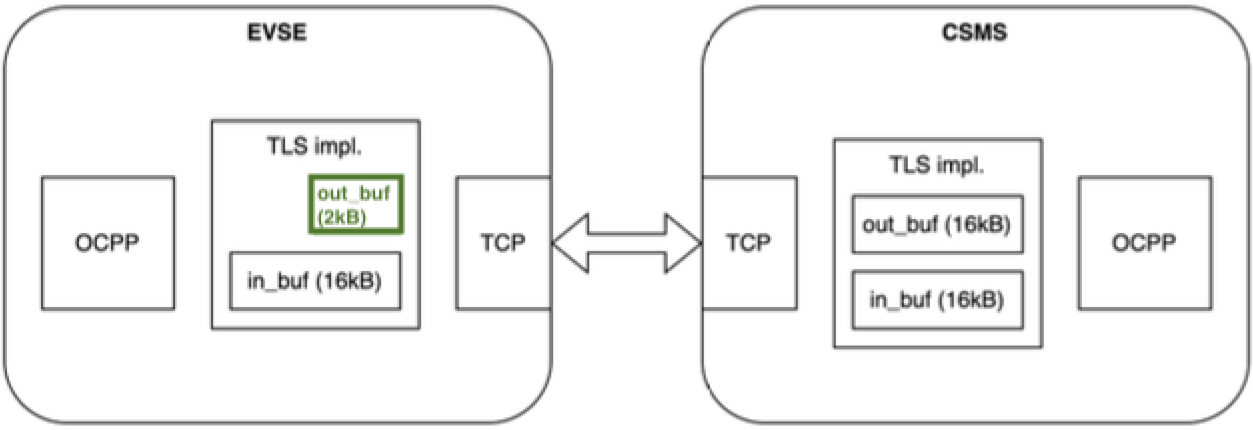

Figure 2. Charging Station allocating a 2 kB TLS output buffer

4.4. Data communication and OCPP messages sizes

The data communication usage of a charging station is highly dependent on its usage profile and configuration. A residential charging station with one charging session per day generates significantly less data traffic than a busy fast charger. Similarly, some chargers may be configured to provide meter values every 15 minutes, while a fast charger might be set to do this every 30 seconds. Therefore, it is not possible to provide a general estimate of data transmission without specifying the usage profile of the charging station.

There are no standardized usage profiles for charging stations that allow for an estimated data usage. To offer some insight into the size of OCPP messages, data logs from official OCPP certification tests of 15 charging stations were analyzed. A total of 931 test cases were executed, resulting in the transmission of 32,636 messages.

Example of an OCPP message

```
 [2,"38a28818-3a91-4e82-a03a-fbd992a92b11", "TransactionEvent",
{"eventType":"Started","evse":{"connectorId":1,"id":1},"idToken":{"idToken":"
00abf91f","type":"ISO14443"},"seqNo":0, "timestamp":"2024-04-
23T02:06:02.444Z","transactionInfo":{"chargingState":"Idle","transactionId":"
a32ad195-e467-4423-ae0b-61e1e617f1b1"},"triggerReason":"Authorized"}]
```

From this data, the following statistics were derived:

- Smallest message length: 25 characters
- Average message length: 235 characters
- Largest message length: 64,907 characters

NOTE The largest message resulted from one charging station sending an entire device model report as a single NotifyReport message, rather than breaking it into smaller chunks as is typically done.

The majority of OCPP messages (~95%) are smaller than 500 characters. The distribution of larger OCPP messages is as follows:

Message size	Message count	Percentage of total (32636)
> 500 chars	1334	4%
> 1000 chars	306	0.94%
> 2000 chars	148	0.45%
> 4000 chars	34	0.10%

5. Minimizing persistent memory usage

5.1. Persistence of charging profiles

OCPP 2.0.1 requires that charging profiles are stored persistently. If a CSMS sends frequent updates of a charging profile, this will eventually wear out flash memory. This is especially concerning for a charging profile of type TxProfile, because that is sent for every transaction. A similar concern applies to charging profile of type ChargingStationExternalConstraints, which originate from an external actor, such like an energy management system.

For this reason, the requirement for persistence of TxProfile and ChargingStationExternalConstraints charging profiles has been removed from OCPP 2.1, reducing the amount of persistent memory needed.

5.2. Minimizing device model size

The OCPP device model is a repository of configuration variables (stored in controller components) and components that represent their physical counterparts in the charging station.

A substantial amount of ROM and persistent memory can be saved if the device model is implemented without utilizing an embedded database, and if only mandatory components are supported. For the limited functionality of resource-constrained charging stations, this is a viable option.

Of the more than 50 required variables for OCPP 2.0.1, only 19 require to be writable by CSMS and need to be stored in persistent memory. These are configuration variables that will not be changed often and can therefore easily be stored in a simple file without requiring an embedded database. The remaining variables are either read-only (preconfigured) values that can be part of the firmware, or are real-time state values, like "Availability", that do not require to be stored.

5.2.1. Mandatory charging infrastructure components

Charging infrastructure components refer to physical components that are used for charging:

- ChargingStation
- EVSE
- Connector

The variables that are required by the OCPP specification for these components can all be treated as read-only variables, which means that their value can be hard-coded in the implementation, either as a fixed value or as a value that is reported based on the system state.

The SupplyPhases of an EVSE can be hard-coded in a configuration file, because it will not change during operation. The AvailabilityState (Available, Occupied, etc.), will change during operation, but the current state can readily be reported by the application at any time. There is no need to store that in a database.

ChargingStation

- AvailabilityState: reports current state from firmware (read-only)
- Available: set to true (read-only)
- SupplyPhases: preconfigured value reported from firmware (read-only)

EVSE

- AvailabilityState: reports current state from firmware (read-only)
- Available: set to true (read-only)
- SupplyPhases: preconfigured value reported from firmware (read-only)
- Power: only maxLimit is required, but actual value can also be reported from firmware (read-only)

Connector

- AvailabilityState: reports current state from firmware (read-only)
- Available: set to true (read-only)
- SupplyPhases: preconfigured value reported from firmware (read-only)
- ConnectorType: set to fixed value as part of firmware (read-only)

5.2.2. Controller components

This section lists the device model components that are required to be implemented even in a minimal implementation. The majority of these variable can be read-only and can therefore be hard-coded in the firmware. The variables that must be configurable by CSMS are shown in **boldface**.

AlignedDataCtrlr

The AlignedDataCtrlr is required for the Core profile, but in most cases only the use of SampledDataCtrlr will be enough. Its variables are required to be Read/Write, but can initially be set to values that will cause no MeterValues to be reported for aligned data measurands. This means that:

- Available: set to true
- **Interval**: set to 0 (no aligned data to be reported)
- **Measurands**: set to empty
- **TxEndedMeasurands**: set to empty (no aligned data at end of transaction)
- **TxEndedInterval**: set to 86400 (24 hours) (Exact value irrelevant if TxEndedMeasurands is empty)

AuthCtrlr

The AuthCtrlr has three required parameters:

- AuthorizeRemoteStart: can be read-only and set to a fixed value, depending on whether remote start is supported or not.
- LocalAuthorizeOffline, LocalPreAuthorize: can be read-only. Value is irrelevant, because local authorization cache or authorization list are not supported in a minimal implementation.

ClockCtrlr

The ClockCtrlr is only required to present the current time and time source.

- DateTime: a read-only value that reflects current clock time.
- TimeSource: read-only and set to Hearbeat, because a minimal implementation only supports heartbeat as time source.

DeviceDataCtrlr

Purpose of the DeviceDataCtrlr is to report limits on messages from a CSMS for device model variables, which can potentially be very large.

- ItemsPerMessage[GetReport/GetVariables/SetVariables]: read-only, set to a fixed small enough value, e.g. 1.
- BytesPerMessage[GetReport/GetVariables/SetVariables]: read-only, set to a fixed small enough value, e.g. 300.

OCPPCommCtrlr

The OCPPCommCtrlr has a set of required variables, some of which must be writable by CSMS. This can be stored in a file that holds the configuration settings.

- FileTransferProtocols: is read-only and set to the supported value(s).
- MessageTimeout[Default]: is read-only and set to configured value.
- **MessageAttemptInterval**[TransactionEvent]: is read-write and supported.
- **MessageAttempts**[TransactionEvent]: is read-write and supported.
- **NetworkConfigurationPriority**: is read-write and supported.
- **NetworkProfileConnectionAttempts**: is read-write and supported.
- **OfflineThreshold**: is read-write and supported.
- **ResetRetries**: is read-write and supported.
- UnlockOnEVSideDisconnect: can be read-only and set to supported value.

SampledDataCtrlr

The SampledDataCtrlr defines the measurands to report during a transaction. The values must be writable by CSMS and therefore need to be stored in a configuration file.

- **TxEndedInterval**: : is read-write and supported.
- **TxEndedMeasurands**: is read-write and supported.
- **TxUpdatedInterval**: is read-write and supported.
- **TxUpdatedMeasurands**: is read-write and supported.

SecurityCtrlr

The SecurityCtrlr holds properties related to the websocket connection and certificaties.

- CertificateEntries: can be read-only set to number of supported certificates.
- **OrganizationName**: read-write and set by CSMS.
- SecurityProfile: can be read-only and reflects current security profile.
- **Identity**: is not required, yet recommended to be supported as a read-write variable, because it is part of the connection URL to CSMS.

SmartChargingCtrlr

Smart charging is not part of a basic implementation, but it may be desired to include in a minimal implementation in certain cases. The following is a minimal SmartChargingCtrlr:

- Available: set to true or false (read-only)
- Entries[ChargingProfiles]: set to number of supported charging profiles, e.g. 1 (read-only)
- **LimitChangeSignificance**: needs to be writable by CSMS
- PeriodsPerSchedule: set to number of periods supported, e.g. 3 (read-only)
- ProfileStackLevel: set to highest stack level supported, e.g. 0 for only 1 level (read-only)
- RateUnit: set to rate unit supported, e.g. A (read-only)

TxCtrlr

The TxCtrlr defines start and stop point of a transaction. For a minimal implementation this is best set to PowerPathClosed, which is the same condition that is used in OCPP 1.6.

- **EVConnectionTimout**: must be writable by CSMS
- StopTxOnEVSideDisconnect: read-only, set to true
- **StopTxOnInvalidId**: must be writable by CSMS
- TxStartPoint: can be set to read-only and recommended value PowerPathClosed.
- TxStopPoint: can be set to read-only and recommended value PowerPathClosed.

6. Implementation notes

6.1. Transaction model

OCPP 2.0.1 expands upon the 1.6 transaction model by introducing (among other things) flexible start and stop points and significantly expanding specific requirements for individual use cases. While this improvement increases the specification’s flexibility and precision, it also complicates the process of translating the specification into concrete implementations and defining reasonable abstractions and requirements for operation-level request handlers (for example: collecting all use case requirements into a single "onRequestStartTransactionRequest" handler within an implementation). To address this challenge, embedded manufacturers are encouraged to reference existing open-source implementations and associated designs as potential models for reuse.

In this section we present one possible approach to implementing OCPP 2.0.1 transaction handling with minimal memory usage. The implementation notes will focus on an approach only targeting the minimum recommended support from Section E. Transactions; that is TxStartPoint and TxStopPoint both set to PowerPathClosed with no support for other transaction start/stop points.

6.1.1. Authorization

An authorization instance represents one of the following:

- A RequestStartTransactionRequest sent from the CSMS
- An RFID tap on the station not already associated with a transaction
- A custom vendor-specific "autostart" extension

When any of these operations occur, a authorization instance is created, which will:

- Send out an AuthorizeRequest if necessary to authorize the transaction with the CSMS
- Be matched against a plugged-in connector to start a transaction
- Expire after a timeout (such as ConnectionTimeOut)

The authorization instance is removed when:

- It is used to start a transaction, or
- It is replaced by a more recent similar request

Note: it may be reasonable for an implementation to only allow a authorize operation on the station as a whole (so that an RFID tap or a RequestStartTransactionRequest would replace any earlier attempts), or to allow multiple requests to co-exist in a limited fashion. For example, it may be reasonable for two RequestStartTransactionRequests for different EVSE IDs (on a multi-connector charger) to co-exist with each other, but it would likely be confusing to allow two RFID taps or an RFID tap and a RequestStartTransactionRequest with no EVSE ID to co-exist with each other.

6.1.2. Transactions

A transaction represents an on-going (persistent) operation that has been resolved to a single connector. In this model transactions represent authorised charging sessions and while a transaction instance is active energy is offered to the vehicle (according to the active power management rules).

While transactions are running various transactions events are sent out in response to the following events:

- When a transaction starts/stops
- When the charging status changes (for example from Idle to Charging or vice-versa)
- When a transaction is de-authorised by the CSMS
- When meter value readings are added (based on the OCPP configuration)

All of these events must be persisted and replayed to the CSMS in the event the charger goes offline or a power loss occurs. An effective way to do this without dramatically impacting transaction handling is to push transaction events into a **pending message queue** which queues those messages and delivers them to the CSMS, retrying and persisting as necessary.

6.1.3. Pending message queue

Pending messages can be accumulated in a separate module for storage/retries (see, for example: **E11**). This is useful to separate the complexity of the transaction state machine from:

- Sending messages
- Retrying historic messages
- Discarding old data due to memory or storage space limitations
- Persisting historic messages to prevent loss during power outages

One approach to this type of separation is the following:

- Augment pending (transaction) messages with a transaction ID and a "removal priority"
- Remove messages to save space as per E04.FR.08, E11.FR.05, and E12.FR.05:
    - First remove meter value data in the middle of a transaction (preserving the first and last meter value as long as possible)

        - Then remove the first and last meter value

Note that this approach typically comes with per message overheads on the order of hundreds of bytes per message. This can rapidly eat into available heap/flash space when attempting to store these records. One approach that was found to be effective in practice was to compress the data using standard gzip compression in memory into reasonable sized blocks. This dramatically improved storage (record size was reduced from roughly 600 bytes uncompressed to roughly 45 bytes compressed) at the cost of some processing time and fixed heap costs while compressing/decompressing (for gzip internals) when attempting to process/remove records (required recompression of the block). The results of one such implementation was the following:

- ZLib window bits: 11
- ZLib memory level: 1
- Compression overhead: ~15k heap
- Decompression overhead: ~7k heap
- Average decompressed message size: 640.1 bytes
- Average compressed message size: 51.6 bytes

Other approaches might be:

- Binary encoding of messages internally
- Custom delta encoding of data in stream

These approaches may offer a lighter message-specific implementation that may be less resource intensive or may achieve improved compression ratios.

6.2. Supporting HTTPS in FirmwareUpdate, GetLog, or third-party connections

The 2.0.1 specification allows a manufacturer to support a variety of secure and insecure protocols that it accepts as a communication channel for FirmwareUpdate/GetLog connections, such as HTTP, HTTPS, FTP, FTPS, and SFTP. It is clearly beneficial to use common secure protocols here, particularly because both firmware updates and log messages may contain sensitive data — however that choice often comes with significant additional costs in terms of memory usage.

Including a FTPS or SFTP library may involve attempting to pull in large popular open source libraries like libcurl that can be difficult and expensive to integrate into an embedded environment, while HTTPS support often raises questions about certificate management overhead, complexity, and so on, especially in resource constrained lite devices. Note that endpoints provided in those requests (specifically those based on TLS like HTTPS or FTPS) may not use TLS certificates signed by root CAs provided to the charger to secure its CSMS connection in security profile 2/3, and the specification has not yet defined how a manufacturer should secure these TLS connections.

One alternative that was found to be effective is to support HTTPS connections to these "external" URLs and secure the connections using the certificate bundle support provided by ESP-IDF/Mbed-TLS. This was found to effectively allow secured HTTPS connections with the same level of complexity as supporting HTTP connections, no significant heap overhead, and only a small impact on binary size (approximately 62 KiB, which was small next to the reference firmware sizes of roughly 1 MiB - 1.5 MiB). Similar approaches at varying levels of complexity can likely be adapted to other embedded platforms supporting the Mbed-TLS library (depending on the platform’s level of support for this feature). It’s also worth noting that this approach may be applicable for securing other third-party HTTPS connections a charging station may need to establish outside of the OCPP protocol.

The following settings were used to enable certificate bundle support on a reference ESP32 implementation:

- CONFIG_MBEDTLS_CERTIFICATE_BUNDLE=y
    - Enables the CA bundle
- CONFIG_MBEDTLS_CERTIFICATE_BUNDLE_DEFAULT_FULL=y
    - Embeds a complete list of Mozilla’s NSS root certificates
    - Impact on binary size: ~64057 bytes
- config.crt_bundle_attach = esp_crt_bundle_attach;
    - Uses the CA bundle to verify the server’s certificate in the standard ESP-IDF HTTPS client

IMPORTANT

CA bundles should not be used to secure the charging station’s OCPP connection to a back-end in security profile 2/3. Trusting a large number of CA authorities in security profile 2/3 is not considered secure.

References

- [OCPP-Part2] OCPP 2.0.1 Part 2 - Specification
- [OCPP-Part5] OCPP 2.0.1 Part 5 - Certification Profiles
- [OCPP-Part6] OCPP 2.0.1 Part 6 - Test Cases
- [OCPP-16] OCPP 1.6
- [Sec-WP] OCPP 1.6 Security Whitepaper (3rd edition)
- [MicroOCPP] OCPP 1.6/2.0.1 protocol stack, https://github.com/matth-x/MicroOcpp
- [OpenOCPP] OCPP 1.6/2.0.1 implementation by ChargeLab, planned to become open source

APPENDIX A: Summary of messages per section

Table 2. Minimum message set

Section	Use Cases	Messages
A. Security	• A00 Security Profile 1 & 2 • A01 Update CS password • A04 Security Event	SetVariables, SecurityEvent
B. Provisioning	• B01/B02/B03 Cold Boot - Accepted, Pending, Rejected • B04 Offline Idle • B05 Set Variables • B06 Get Variables • B07 Get Base Report • B09 Set Network Profile • B10 Migrate to New CSMS • B11/B12 Reset Charging Station	BootNotification, SetVariables, GetVariables, GetBaseReport, NotifyReport, SetNetworkProfile, Reset
C. Authorization	• C01, C02, or C04 Authorization	Authorize
(D. Local Authorization List)	-	
E. Transactions	• E01 Start Transaction (PowerPathClosed) • E05 Start Transaction - id not accepted • E06 Stop Transaction (PowerPathClosed) • E07 Transaction stop by idToken • E08 Transaction stop while offline • E09 Transaction Stop - cable disconnect on EV • E11 Connection Loss during transaction • E12 Inform of offline transactions • E13 Transaction message not accepted	TransactionEvent, GetTransactionStatus

Section	Use Cases	Messages
F. Remote Control[1]	- (F01 Remote Start - Cable First) - (F02 Remote Start - Start First) - (F03 Remote Stop) - (F05 Remote Unlock) - (C05 Authorization CSMS Initiated Transactions)	RequestStartTransaction, RequestStopTransaction, UnlockConnector
G. Availability	- G01 Status Notification - G02 Heart Beat - G04 Change Availability Charging Station	StatusNotification, Heartbeat, ChangeAvailability
(H. Reservation)	-	
(I. Tariff and Cost)	-	
J. Meter Values	- J02 Transaction-Related Meter Values	TransactionEvent, MeterValues
(K. Smart Charging)*	- (K01 Set Charging Profile) - (K02 Central Smart Charging) - (K10 Clear Charging Profiles)	(SetChargingProfile), (ClearChargingProfiles), (GetCompositeSchedule), (GetChargingProfiles), (ReportChargingProfiles)
L. Firmware Management	- L01 Secure Firmware Update, - (L02 Non-Secure Firmware Update)	UpdateFirmware, FirmwareStatusNotification
M. Certificate Management	- M03 Retrieve list of available certificates - M04 Delete a certificate - M05 Install CA certificate	InstallCertificate, GetInstalledCertificateIds, DeleteCertificate
N. Diagnostics	- N01 Retrieve Log Information	GetLog, GetCustomerInformation, ClearCustomerInformation
(O. Display messages)	-	
(P. Datatransfer)	-	

* *Not part of Core profile, but possibly desired functionality in a minimal implementation*

APPENDIX B: Case study MicroOCPP

<This appendix will be updated in a later version with results from MicroOCPP implementation>

APPENDIX C: Case study OpenOCPP

<This appendix will be updated in a later version with results from OpenOCPP implementation>