Migrating Charging Stations

v1.0, November 2025

Table of Contents

1. Introduction 2
2. What needs migrating? 3
3. Outline of migration steps 4
4. OCPP 1.6 migration 7
5. OCPP 2.x migration 8
6. Common hurdles when migrating 11
7. Conclusion 13
APPENDIX A 14
    Case study: GreenFlux - Eneco Migration 15
APPENDIX B 18
    Strategic Migration of 100.000+ EV Chargers from Shell to Last Mile Solutions for 50five 19
APPENDIX C 22
    Seamless Charger Network Migration — Lessons from EVConnect & ChargerHelp with BTC POWER Network Transition 23
APPENDIX D 27
    Successful Migration Case Study: Kople’s Transition to the Driivz Platform 28

OCA White Paper

Author: Open Charge Alliance Acknowledgements: Thank you to ChargerHelp, EV Connect, GreenFlux, Last Mile Solutions and Driivz for providing case studies of real-life, large-scale migrations included in the appendices.

Disclaimer

This document includes recommendations based on experiences of our members. One should study its requirements, configuration and needs and should not take anything from this document for granted. Open Charge Alliance will not be liable for any damages, losses or causes of action of any nature arising from any use of this document.

Chapter 1. Introduction

Charging stations that require billing or registration of charging sessions are typically managed by a charging station operator (CSO), also referred to as a network operator. A CSO's network often comprises various brands of charging stations, all configured to connect to the CSO's backend system, known as the charging station management system (CSMS).

Charging stations are expected to stay in operation for years, oftentimes more than a decade. At the same time, this emerging industry is dynamic and volatile, and is not yet settled. Network operators are switching to different, better management platforms or network operators go out of business entirely. These charging stations are perfectly capable of continuing to operate, so they need a new home: they need to migrate to a new CSMS of another charging station operator (CSO).

Migrating charging stations is a complex process, especially when it involves hundreds or thousands of units that must switch to a new backend while minimizing downtime. This white paper explores the key considerations and steps involved in such a migration, focusing exclusively on charging stations compliant with the Open Charge Point Protocol (OCPP). However, many of the principles discussed—particularly those unrelated to OCPP—also apply to stations using proprietary protocols.

This methodology described in this paper is valid in the following scenarios:

- **In-company migration**: A CSO deploys a new management platform and migrates their charging stations from their old to their new CSMS
  (In that case the former and new CSO are the same party).
- **Cross-company migration**: A new CSO onboards the charging stations of the former CSO to their CSMS
  (The situation where either the former CSO or the manufacturer are not providing support, is addressed in Common hurdles when migrating).
- **Individual customer migration**: An individual customer wants to change their CSO but still wants to keep their charger.

At the end of the paper we will present several case studies of real life network migrations in Europe and the US. One thing stands out in these case studies: the use of OCPP certified CSMS and charging stations greatly simplifies the migration to a different network.

- Appendix A: Case study: GreenFlux - Eneco Migration
- Appendix B: Strategic Migration of 100.000+ EV Chargers from Shell to Last Mile Solutions for 50five
- Appendix C: Seamless Charger Network Migration — Lessons from EVConnect & ChargerHelp with BTC POWER Network Transition
- Appendix D: Successful Migration Case Study: Kople's Transition to the Driivz Platform

Chapter 2. What needs migrating?

A successful migration requires addressing both the physical and digital components of the charging infrastructure. Below, we outline the primary elements that must be transferred or reconfigured.

This paper refers to the existing network to which the charging station are currently connected, as the "old CSMS" or "old CSO", and the network to migrate to, as the "new CSMS" or "new CSO".

2.1. Charging stations

Charging stations are the core assets in a migration. Several aspects of their configuration and physical setup must be updated:

Network configuration for backoffice connection

Each station must be reconfigured to communicate with the new CSMS, typically by updating its network settings to point to the new backend's URL or IP address.

SIM cards

For stations relying on cellular connectivity, SIM cards may need to be replaced or transferred to a new provider contracted by the receiving CSO.

QR/NFC stickers

For public charging stations user-facing identifiers like QR codes or NFC tags, which link to the CSO's payment or authentication system, must be updated or replaced.

Payment service provider contracts

When charging stations with a payment terminal are involved, the contract with the payment service provider will have to be updated for the new CSO.

Payment terminal configuration

The configuration of the payment terminal needs to be updated for the new CSO, e.g. new merchant address.

Signage

Physical signage displaying the old CSO's branding or instructions may need to be revised to reflect the new operator.

2.2. User accounts

User accounts tied to the old CSMS must also be migrated. This includes transferring user data—such as payment details, charging history, and preferences—to the new system, ensuring a seamless experience for end users.

Chapter 3. Outline of migration steps

Migrating charging stations requires a structured approach to ensure compatibility, minimize disruption, and maintain operational continuity. The following plan outlines the key phases of the process.

3.1. Test each charging station model

Before a full-scale migration, each model of charging station in the network must be tested for compatibility with the new CSMS. The charging stations in operation may have several different software versions. The former CPO can indicate what the software version of each station is and what functions and configurations they have.

OCPP compatibility with CSMS

Not all OCPP implementations are created equal. Unless both charging station and CSMS implementation have an official OCPP certification, it is essential to test compatibility between the two.

- Test firmware for OCPP compatibility with new CSMS: Verify that the station's firmware supports the OCPP version (e.g., 1.6 or 2.0.1) used by the new CSMS and run tests to check interoperability.
- Identify and resolve any discrepancies in protocol implementation. The charging station manufacturer may have to update the firmware to resolve issues.
- Develop an adapter if necessary: If compatibility issues arise, a software adapter may need to be developed to bridge communication between the station and the new backend.

Network configuration approach

A charging station has specific configuration settings that control to which CSMS it needs to connect and how. This is called "network configuration".

Determine which process of updating the network configuration is applicable to this charging station model. It will be one of the following methods:

- Via network configuration commands: OCPP commands (e.g., `ChangeConfiguration` /`SetNetworkProfile`) can be used to remotely update the station's connection settings. (This requires assistance from the former CSO).
- Via firmware update: A firmware update is needed that includes the new network settings. (This requires assistance from the manufacturer).
- Via custom update script: A script tailored to the station's hardware/firmware needs to be developed and deployed for automated reconfiguration.
- Via manual (on-site) update: The station cannot be updated remotely. Dispatch a technician to manually adjust settings.

Transfer of SIM card

Charging stations utilize a modem with a SIM card to connect to the internet via a cellular network.

- Test transfer of SIM card to new CSO: Confirm that SIM cards can be reassigned to the new CSO's cellular provider without interrupting connectivity. If reassignment is not possible, the SIM card will have to be

replaced, which means that the station will have to be visited by service personnel.

- Test change or removal of APN: Validate that Access Point Name (APN) settings can be updated or removed as needed to align with the new provider's network.

Update payment terminal contract and configuration

- Test payment terminal configuration: Test updating of payment terminal configuration to match the new payment service provider contract. Verify payment process.

3.2. Transfer old CSMS data

Data from the old CSMS must be migrated to ensure continuity for both the operator and EV drivers.

Charging station data

- Provision new CSMS with all to-be-migrated charging station data: Transfer details such as station IDs, locations, and configurations to the new backend. For roaming interfaces the external name of the stations' EVSEs (EVSEID) will have to change for a new CSO.

Roaming agreements

- Enable additional roaming contracts and interfaces: Activate roaming agreements with other networks (e.g., via OCPI) to maintain interoperability for EV drivers.

EV driver accounts

- Register in new CSMS: Import EV driver account data into the new system, ensuring all profiles are accurately recreated. This step is not needed if the CSO does not act as an MSP, i.e. if CSO does not have direct contracts with EV drivers.

ID token whitelists

- Copy the local authorization lists (whitelists), if any, from old to new CSMS. The mechanism to do this is proprietary to each CSMS.

3.3. Migrate charging stations

To minimize disruption, migrate stations in controlled batches rather than all at once. For each batch perform the following steps:

Transfer SIM cards

- Replace or reassign SIM cards in each batch, testing connectivity with the new CSMS after each transfer.

Update charging station network configuration

- Adjust the network settings for each batch based on the station's OCPP version. Detailed information on this is provided in the chapters OCPP 1.6 migration and OCPP 2.x migration.

Update charging station other configuration parameters

- Configure any other configuration parameters that are relevant in the new network.

Install ID token whitelist

- Install the local authorization list (whitelist) at stations that use it.

Redirect or replace QR/NFC code stickers

- Update QR codes and NFC tags to link to the new CSO's authentication or payment system. This may involve reprinting and affixing new stickers or redirecting existing codes via a backend update.

WARNING	Fixed QR/NFC codes are sensitive to fraud. Switch to dynamic QR/NFC codes on a display if possible.

Update on-site signage where needed

- If local signage is involved that needs updated for the new CSO, perform a site visit to replace signage.

Chapter 4. OCPP 1.6 migration

OCPP 1.6 does not prescribe how the network connection is configured. Ideally, it is all configured via configuration keys, in which case the configuration can be updated via `ChangeConfiguration` messages. The configuration key names are not standardized. Check the manufacturer's documentation to learn which configuration keys are used to configure the network connection. Configuration keys to look for (with commonly used names), are:

- CSMS URL, e.g. "OcppCsmsUrl" or "CSMSURL"
- Basic authentication password, e.g. "BasicAuthPassword" or "AuthorizationKey"
- Security profile, e.g. "SecurityProfile"
- CSO name, e.g. "CpoName"

If the connection cannot be configured via configuration keys, then support from the manufacturer will be needed. Some manufacturers have direct access to their charging stations via a proprietary port through which configuration changes can be made. In some cases the configuration details are hard-coded in the firmware or exist in a package that can be installed via a firmware update (`UpdateFirmware` message). In both cases involvement by the equipment manufacturer is required.

Worst-case, if there is no way to remotely update the configuration, a site visit will be required to locally update the configuration via a direct connection to the station.

WARNING	Several separate messages will have to be sent to complete a configuration. If the network connection is lost while a configuration is only half complete, the charging station may not be able to connect to a CSMS anymore.

Chapter 5. OCPP 2.x migration

As of OCPP 2.0.1. the OCPP specification contains use cases that describe network configuration and migration to a new CSMS. A specific message has been introduced for setting the network connection configuration: `SetNetworkProfile`. This is described in the specification in use cases "B09 - Setting a New NetworkConnectionProfile" and "B10 - Migrate to New CSMS".

5.1. Migrating with security profile 2

Security profile 2 uses TLS with server certificates and basic authentication for the charging station. This is the minimum security profile for production environments. Security profile 1 with basic authentication only, is not considered sufficiently secure in production environments (unless used in a trusted network with VPN or APN), because the authentication credentials are sent as plain text.

The following list outlines the steps to be taken.

Step 1. **Install the root certificate of new CSMS in charging station**

Installation of a root certificate is described in use case "M05 - Install CA Certificate in Charging Station". The CSMS root certificate is installed in the charging station via the message:

```
"InstallCertificateRequest": {
    "certificateType": "CSMSRootCertificate",
    "certificate": "<certificate>" }
```

If the configuration variable SecurityCtrlr.AdditionalRootCertificateCheck = true, then the charging station will only accept the new CSMS root certificate if it has been signed with its current CSMS root certificate. This prevents the installation of rogue certificates by an attacker.

Step 2. **Set the network connection profile for the new CSMS**

A charging station has at least two network profile slots, e.g. "1" and "2". If the "old" CSMS connection is defined in slot "1", then the "new" CSMS connection can be set in slot "2" as follows:

```
"SetNetworkProfileRequest": {
    "configurationSlot": 2,
    "connectionData": "<NetworkConnectionProfileType>" }
```

The *<NetworkConnectionProfileType>* is a structure containing all fields that are needed to set up a connection to the new CSMS. For example, the field *ocppCsmsUrl* contains the URL of the new CSMS and the field *securityProfile* will be set to 2 for security profile #2.
The *<NetworkConnectionProfileType>* element does not include the fields *identity* and *basicAuthPassword* in OCPP 2.0.1. These fields are used as username and password for the websocket connection. This means that if the new CSMS uses a different username/password for basic authentication (security profile 1 and 2) than the old CSMS, then these fields will have to be set explicitly via a `SetVariablesRequest` message.

> OCPP 2.1 has extended the `SetNetworkProfileRequest` to include the fields *identity* and

basicAuthPassword as part of the network connection profile. The advantage is not only that it is no longer needed to issue `SetVariablesRequest` messages to change these values, but it also ties these fields to the network connection profile. This allows for different username/password combinations in network connection profiles for old and new CSMS.

Step 3. **Set the network configuration priority**

The device model variable OCPPCommCtrlr.NetworkConfigurationPriority contains a list of network connection profiles that will be tried in sequence in order to establish a connection. Set the value to "2,1" via:

```
"SetVariablesRequest": {
    "component": "OCPPCommCtrlr",
    "variable": "NetworkConfigurationPriority",
    "attributeValue": "2,1" }
```

This instructs the charging station to first try to connect to the new CSMS, and if that fails, connect to the old CSMS again.

NOTE

Connecting to network connection profile "1" (the old CSMS) will not be successful anymore if the *identity* or *basicAuthPassword* were changed for connecting to the new CSMS. In order to avoid bricking the device, there is a requirement that states that, if none of the network connection profiles were successful, the charging station needs to fall back to the configuration values that were used for the last successful connection.

Step 4. **Reset the charging station**

CSMS instructs the charging station to reset itself after which it will connect to the new CSMS using connection profile "2". After receiving and responding to the BootNotificationRequest from the charging station, CSMS will send a GetBaseReportRequest(FullInventory) to get the full device model with all capabilities and configuration variables from the charging station.

Once the charging station has successfully migrated to the new CSMS (i.e. network connection profile in slot "2"), the network connection profile for the old CSMS in slot "1" should be removed.

5.2. Migrating with security profile 3

With security profile 3 the charging station no longer uses basic authentication. Instead, the charging station uses a client certificate that has been signed by (the certificate authority of) the CSMS. This behavior is described in use case "A03 - Update Charging Station Certificate" and uses the messages

```
"SignCertificateRequest": {
    "certificateType":  "ChargingStationCertificate",
    "csr": "<csr>" }
```

```
"CertificateSignedRequest": {
    "certificateType": "ChargingStationCertificate",
```

```
    "certificateChain": "<certificateChain>" }
```

A CSMS will only trust charging stations that present a client certificate that has been signed by (the certificate authority of) the CSMS.

In order to migrate with security profile 3 to a new CSMS, all steps from the previous section need to be executed first, except the setting of a basic authentication password.

A charging station from the old network can only connect to the new CSMS if the new CSMS trusts the client certificates that have been signed by the old CSMS. This is a two-step process.

1. **New CSMS verifies that the client certificate is owned by the CSO** (or an organization trusted by the CSO — in this case the old CSO) by checking that the O (*organizationName*) RDN in the subject field of the certificate contains the CSO name. For this to work, the new CSMS needs:
    - to have the public root certificate of the old CSO, and
    - to accept client certificates that have the name of the old CSO in *organizationName* field of the certificate.
2. **New CSMS checks that the certificate belongs to this charging station** by checking that the CN (commonName) RDN in the subject field of the certificate contains the unique serial number of the charging station.

Once a charging station has succesfully connected to the new CSMS, the new CSMS can set the configuration variable SecurityCtrlr.OrganizationName to the proper name of the new CSO and instruct the charging station to generate new client certificates and have them signed by the new CSMS, as per use case "A02 - Update Charging Station Certificate by request of CSMS".

Chapter 6. Common hurdles when migrating

A seamless migration can be achieved when the old and new CSOs collaborate effectively and when support from the charging station manufacturer is accessible. However, this may not always be the case.

6.1. Interoperability issues

One of the most prevalent challenges encountered during the migration of charging stations to a different backend is a lack of interoperability. This issue arises when the charging station and the CSMS each have slightly differing interpretations of the OCPP standard. Interoperability issues can be mitigated if both the CSMS and charging stations are OCPP certified. Such certification can be easily verified on the Open Charge Alliance website.

When interoperability issues arise, two potential solutions can be pursued:

1. Request the charging station manufacturer to update the station's firmware to ensure compatibility with the new CSMS.
2. Adapt the new CSMS software to work with the charging station's OCPP implementation.

The choice of solution will be dictated by the specific circumstances, including the availability of resources for firmware or backend development.

6.2. Lack of support from the charging station manufacturer

If the charging station manufacturer has ceased operations or is unwilling or unable to provide any support, a firmware update cannot be requested to resolve interoperability issues.

In cases where the charging station operates on OCPP 1.6 and employs proprietary configuration keys (refer to OCPP 1.6 migration), there is a heightened risk that modifying the network configuration will prove challenging without manufacturer support, unless the old CSO possesses detailed technical knowledge of the charging station.

It is therefore important to take care when selecting trusted hardware providers, agree upfront longer term support contracts and set up an ESCROW system for their firmware.

6.3. Lack of support from the old CSO

It is regrettable, yet not uncommon, that the old CSO is unable or unwilling to provide support during the migration process. This situation complicates the migration significantly, as the only online access to the charging stations is through the CSMS of the old CSO.

In certain instances, charging stations may include a backdoor utilized by the manufacturer for remote support. The new CSO can request the manufacturer to utilize this access to modify the station's network configuration, enabling connectivity with the new CSMS. This will need to employ security profile 1 without Transport Layer Security (TLS), as the root certificate of the new CSMS is not installed on the charging station. Once a connection is established, the new CSMS can install its root certificate and upgrade to security profile 2 with TLS.

In the absence of backdoor access, the only remaining option is to visit each charging station on-site and

connect a laptop equipped with the manufacturer's maintenance software via USB or Local Area Network (LAN) to update the connection configuration locally.

Without cooperation from the old CSO, it will not be feasible to migrate all charging station data from the old CSMS to the new CSMS. The new CSO will need to manually enter the identities and properties of each charging station into the new CSMS.

It is therefore important to take care when selecting the CPO, agree upfront that in case of a CSMS migration, the CPO is obliged to cooperate. Additionally, for the needed information for network migration an ESCROW system should be set up.

6.4. SIM card transfer limitations

Charging stations utilize a modem with a SIM card to connect to the internet via a cellular network. The SIM cards are associated with the account of the old CSO. Therefore, the old CSO must request the cellular network provider to transfer the SIM cards to the account of the new CSO.

If this transfer cannot be accomplished, the existing SIM cards will need to be replaced with new ones, necessitating costly visits by service personnel.

The above can be avoided if the charging stations are equipped with eSIMs that support remote SIM provisioning. The term eSIM refers to the physical format of the SIM card. Unlike traditional removable plastic SIMs, an eSIM is a small chip that is permanently soldered into the device during manufacturing. Remote SIM provisioning is responsible for securely storing multiple mobile network operator profiles on the SIM and enabling seamless switching between them Over-The-Air, without the need to replace the physical SIM card.

Chapter 7. Conclusion

Migrating charging stations to a new network is a multifaceted endeavor that demands careful planning, rigorous testing, and precise execution. For OCPP-compliant stations, the process benefits from standardized protocols that facilitate remote management and reconfiguration. However, challenges such as hardware variability, SIM card logistics, and user data migration require tailored solutions.

By following a phased approach—testing compatibility, transferring data, and migrating stations in batches—CSOs can minimize downtime and ensure a smooth transition. As the electric vehicle ecosystem continues to evolve, the ability to adapt and migrate infrastructure will remain a critical capability for operators seeking to maintain reliable, scalable networks.

As shown in this paper, it is important to select trustworthy charging station manufacturers. Over the course of a decade the odds of requiring manufacturer support for a migration cannot be neglected.

APPENDIX A

Case study: GreenFlux - Eneco Migration

Eneco eMobility migrated approximately **3,500** legacy EV charge points from a deprecated vendor platform to **GreenFlux's** hardware-agnostic charging management system. The program balanced three imperatives:

- uninterrupted service for drivers,
- rapid compliance with EU and national price-transparency requirements,
- durable uplift in security and operational control.

Working across diverse OCPP versions—including **1.5 SOAP, 1.5 JSON, and 1.6 JSON**—and two charger generations, the teams executed a phased transition that avoided physical SIM swaps, embedded private APN/VPN security, and resolved protocol customizations that had accumulated over time. The initial cutover successfully moved 3,461 chargers, unifying Eneco's estate on a single, cloud-based back office and enabling ad-hoc charging, real-time data sharing, and future-ready scalability.

Context and Objectives

Eneco eMobility operates a large, mixed network of home and public charge points across the Netherlands, Belgium, and Germany. As its legacy back office approached end-of-life, and as regulators tightened rules around price transparency and ad-hoc access, Eneco faced a strategic choice: either sustain a fragmented environment with rising risk and cost, or consolidate onto a unified, secure platform.

The company selected GreenFlux to serve as the consolidated charging management platform, aiming to preserve customer experience during the transition, strengthen information security, standardize operational processes, and create headroom for growth through acquisitions and new deployments.

The scope centered on a remaining cohort of roughly 3,500 devices still anchored to the deprecated platform. Though modest relative to Eneco's 25,000-plus fleet, this subset was among the most complex because it **spanned older hardware and earlier OCPP implementations** that had seen real-world customizations by a former back-office provider. Any migration strategy therefore had to prioritize compatibility, carefully manage cutover risk, and minimize the need for disruptive fieldwork.

Technical Landscape and Constraints

The estate comprised Generation 2 and Generation 3 AC chargers communicating over multiple protocol variants. Heterogeneity at this layer is common in mature networks, but it narrows the margin for error: messages that pass in a lab may behave differently at scale or when interacting with downstream systems that have learned to expect edge-case behaviors. Eneco and GreenFlux treated this diversity as a first-class design constraint.

They created **representative device cohorts** for integration testing, **validated behavior across OCPP versions**, and compared observed traffic patterns with **protocol specification**s and **back-office expectations**. Where firmware levels or configurations were likely to trigger instability—such as timeouts, incomplete transactions, or metering inconsistencies—the team planned pre-migration remediation so the production cutover would be uneventful.

Connectivity and security requirements layered additional constraints. The teams needed to protect data in

transit while avoiding costly and risky on-site interventions. GreenFlux's ISO-certified platform provided the controls baseline, while collaboration with Eneco's SIM providers enabled private APN and VPN links that could be established **without physically swapping SIM cards**. This approach reduced downtime risk, shortened the critical path, and delivered an immediate improvement in the confidentiality and integrity of charge-point communications.

Program Governance and Execution

The migration unfolded through a phased plan that synchronized technical readiness with operational communications. GreenFlux led the orchestration across six stakeholder groups, setting clear ownership for test cycles, change windows, and incident response. Prior to each phase, the teams confirmed that affected chargers had passed integration tests, that configuration and firmware were at approved baselines, and that monitoring dashboards could detect anomalies quickly. By sequencing cohorts, Eneco maintained service for drivers while steadily increasing the proportion of traffic handled by the new back office.

Equally important was the handling of **protocol customizations** that had accreted over the years. Rather than treat these as defects to be stamped out mid-cutover, the program cataloged them and, where necessary, accommodated them in the new environment to preserve functional parity. In parallel, the teams documented a path to **retire unnecessary deviations** once the fleet was stable, ensuring that the long-term architecture converged on **standards-compliant behavior** without jeopardizing near-term continuity. Cooperation from the former back-office provider helped accelerate this learning curve by providing historical context and assisting with data validation.

Communication with business stakeholders mirrored the technical cadence. Site hosts and customer-facing teams were briefed on the migration schedule, expected outcomes, and contingency plans, with a particular focus on preserving session continuity and billing accuracy. Internally, change windows were chosen to minimize user impact, and **rollback plans were rehearsed** even when confidence was high. This discipline paid dividends: the initial phase brought 3,461 chargers into Eneco's GreenFlux environment with **no reported systemic outage** and with close monitoring to resolve isolated issues rapidly.

Outcomes and Operational Benefits

The migration delivered a unified platform footprint for Eneco's entire charging estate, **simplifying asset management** and strengthening **observability**. Consolidation improved the fidelity of fleet-wide monitoring and analytics, enabling faster detection of communication faults and more consistent application of configuration policies. Just as importantly, the new environment supported features aligned with regulatory expectations, including price transparency and ad-hoc charging. Eneco could share real-time transaction data with customers and partners, improving the clarity of pricing and the accuracy of invoicing.

Security and resilience improved as a matter of course. Private APN and VPN connectivity created a more predictable and protected network perimeter for charge-point communications. The platform's certified controls and modular architecture reduced the likelihood that a compromise or misconfiguration in one area would propagate widely. By **avoiding physical SIM swaps** and other intrusive field actions, the program also lowered operational risk and cost while keeping stations available to drivers.

Financially and operationally, Eneco benefited from platform capabilities that extend beyond simple device connectivity. Smart charging functionality provided opportunities for cost savings, while a single back office

reduced the overhead associated with training, support, and vendor coordination. Because the platform remains hardware-agnostic and supports both **contemporary and legacy OCPP versions**, Eneco is better positioned to incorporate new chargers—whether from organic growth or acquisition—without repeating the fragmentation that prompted this migration.

Lessons for Practitioners

Several themes stand out for CPOs and EMSPs planning similar transitions.

1. Treat **protocol diversity** as a design input rather than an exception: invest in **pre-migration testing** that reflects the true mix of devices and behaviors in the field.
2. **Embed security** into the connectivity fabric from the start; private APN/VPN links and certified back-office controls can materially reduce risk without requiring disruptive fieldwork.
3. Conduct the migration as a **phased program** with crisp ownership and clear communications, aligning technical milestones with business expectations.
4. **Preserve functional parity** during cutover even if it requires short-term accommodation of legacy behaviors, then chart a measured path to retire deviations once stability is assured.
5. View **compliance not merely as a cost but as an opportunity** to unlock features like ad-hoc payments and richer data sharing that deliver value to drivers and site hosts.

Conclusion

The Eneco–GreenFlux migration demonstrates how a complex, multi-party transition can be executed without compromising the customer experience. By foregrounding compatibility across legacy OCPP variants, integrating security by design, and orchestrating a phased roll-out, Eneco consolidated a heterogeneous legacy estate into a unified, future-ready platform.

The result is an operationally cleaner environment that meets current regulatory expectations, strengthens security, and equips the organization for continued growth. As summarized by Eneco's Product Owner IT, Art Speksnijder, the collaboration, commitment, and knowledge provided by GreenFlux were central to a successful migration and will support Eneco's future ambitions for network expansion and scalable operations.

APPENDIX B

Last Mile Solutions

Strategic Migration of 100.000+ EV Chargers from Shell to Last Mile Solutions for 50five

Executive Summary

Following Shell's strategic divestment, ownership and operations of over 100,000 EV chargers were transferred to 50five, a smart energy solutions provider. To ensure a seamless transition and future-proof infrastructure, 50five partnered with Last Mile Solutions, Europe's leading EV charging and energy transaction platform, for the migration and ongoing operations.

Last Mile Solutions led project management, asset and data migration, coordinating across stakeholders and systems. This case study highlights the strategic rationale, technical execution, and outcomes of one of Europe's largest and most complex EV infrastructure migrations, enabled by industry standards like OCPP and Last Mile Solutions' scalable platform.

Background & Strategic Context

Shell exited EV charging operations in select European markets as part of a broader portfolio strategy. 50five acquired Shell's EV assets, including 100.000+ chargers across residential, commercial, and public locations.

To ensure service continuity, 50five selected Last Mile Solutions as its backend and migration partner, based on its expertise in large-scale EV infrastructure, multi-vendor support, and proven platform reliability across Europe.

The migration involved transitioning all charger operations from Shell's legacy systems to Last Mile Solutions' unified backend, requiring deep technical coordination, data transformation, and operational readiness.

Objectives

The migration project was guided by a set of strategic and technical objectives:

- Service Continuity: Ensure uninterrupted service for EV drivers and partners throughout the migration.
- Technology Readiness: Ensure the Last Mile Solutions system is ready to scale and operate effectively, handling the increased volume of customers, chargers, and data post- migration.
- Platform Readiness: Ensure the Last Mile Solutions platform is fully prepared to support the migration, with all required features, functionalities, and system configurations in place.
- Data Readiness: Successfully create, validate, and map data for over 100.000 chargers and associated customer records, ensuring no data loss or integrity issues.
- API Readiness: Develop and integrate the necessary APIs between Last Mile Solutions, 50five, and Shell, with full support and testing.
- Hardware & Connectivity Readiness: Validate hardware and firmware compatibility across all charger models and ensure seamless connectivity via telecom providers.
- Operational Readiness: Prepare Last Mile Solutions' customer support and invoicing teams to manage the increased volume of users and assets post-migration.

Challenges

The migration presented several complex challenges:

- Scale & Diversity: Over 100.000 chargers across multiple countries, brands, and hardware types.
- Data Structure Differences: Shell's legacy systems used a fundamentally different data model for customer and payment data, requiring extensive transformation and mapping.
- Data Integrity: Ensuring accurate transfer of charger metadata, user profiles, and transaction history.
- Interoperability: Supporting various OCPP versions and charger brands, while maintaining consistent backend behavior.
- Connectivity & SIM Transition: Coordinating multiple telecom provider transitions and validating SIM card functionality across all chargers.
- Operational Continuity: Avoiding service disruption during migration while maintaining high uptime.
- Customer Communication: Managing expectations and support during the transition.
- Regulatory Compliance: Ensuring data handling and migration meet local regulations (especially relevant across multiple countries).

Migration Strategy

The migration was a joint effort between Shell, 50five, and Last Mile Solutions. Shell and 50five led strategic coordination, setting the scope and pace. Last Mile Solutions, as the backend platform provider, handled operational execution, ensuring technical readiness and onboarding of over 100.000 chargers.

Specialized Workstreams Led by Last Mile Solutions:

- Data & Platform: Developed scripts to validate, transform, and process charger and customer data. Tackled challenges in Shell's legacy structures, especially customer and payment data, using custom tooling and deep system expertise.
- Hardware & Connectivity: Tested charger compatibility across models and firmware. Managed SIM card transitions and endpoint switches with telecom providers to maintain connectivity.
- API Integration: Used APIs for data validation and asset creation. Shell built a dedicated API for endpoint switching. Automation reduced manual effort and ensured system consistency.
- OCPP Standardization: Enabled interoperability and reduced complexity. Despite standardization, diverse charger implementations required extensive validation. Migration at this scale wouldn't be feasible without OCPP.
- Collaborative Governance: Regular meetings, shared documentation, and transparent communication ensured swift issue resolution and efficient decision-making.

Results & Impact

- 100.000+ chargers successfully migrated to Last Mile Solution's platform, with the majority already live and operational.

- 99,98% uptime maintained throughout the migration process.
- Seamless transition for end users, with minimal disruption and no major service outages.
- Improved operational efficiency, including faster transaction processing and reduced support overhead.
- Enhanced platform responsiveness and scalability, supporting future growth and innovation.
- Successful integration of multi-vendor hardware, demonstrating Last Mile Solutions' flexibility and robustness.
- Established a repeatable migration framework for future large-scale transitions.

Key Success Factors

- Highly dedicated and solution-oriented teams across all organizations.
- Last Mile Solutions' technical expertise, especially in data transformation, API integration, and hardware validation.
- Strong collaboration between Shell, 50five, and Last Mile Solutions, with shared ownership and clear communication.
- Agile working methods, allowing rapid adaptation to emerging challenges.
- Custom-built tools and processes tailored to the unique requirements of this migration.
- OCPP standardization, enabling interoperability across diverse charger models and firmware versions.
- Proactive issue resolution, supported by real-time monitoring and validation of scripts.

Lessons Learned

- Close collaboration from the start is essential. Involving field experts early helps avoid delays.
- Data quality and structure must be assessed and addressed proactively, especially when migrating from legacy systems.
- Sufficient time for testing and problem-solving is critical to avoid rushed decisions and ensure stability.
- Customer communication is key. Clear messaging reduces support load and builds trust.
- OCPP compatibility varies. Technical flexibility is needed to handle edge cases.
- Real-time monitoring enables faster detection and resolution of issues.
- Platform flexibility ensures long-term scalability and adaptability.

APPENDIX C

Seamless Charger Network Migration — Lessons from EVConnect & ChargerHelp with BTC POWER Network Transition

Overview

In early 2025, a **prominent utility company** faced a pressing challenge: migrate 76 BTC POWER DC fast chargers (DCFCs) from the **Shell Recharge** network to **EV Connect** before the Shell Charge Management System CMS was shut down on **April 30**.

To meet this deadline, the utility engaged **ChargerHelp** to execute field operations and troubleshooting, and **EV Connect** to serve as the new (CMS). The collaboration between ChargerHelp, EV Connect and BTC POWER (both of whom are Open Charge Point Protocol (OCPP) certified), and the utility revealed not only best practices—but the **critical importance of OCPP compliance in making migrations scalable and efficient**.

Project Snapshot

Project Phase	Details
Scope	76 BTC POWER DCFC chargers
Old CMS	Shell Recharge
New CMS	EV Connect
Field Operations	Led by ChargerHelp
Deadline	April 30, 2025
Hardware	BTC POWER Chargers

Why This Network Migration Mattered

The [Prominent utility] project wasn't just about flipping a switch—it highlighted what's involved in maintaining a stable, future-proof EV infrastructure in a rapidly evolving ecosystem. With the Shell Recharge CMS shutting down, they needed a partner ecosystem that could:

- Preserve charger uptime
- Minimize operational disruption
- Navigate complex vendor relationships
- Execute quickly and confidently
- Manage to an affordable and agreed upon budget
- Deliver on their long-term needs as well as, or better than, any leading provider in the industry.

Thanks to **OCPP compliance** and a phased, cross-team approach, the migration was completed and the utility is charging ahead with their new charging platform partner.

The Value of OCPP in Charger Migrations

OCPP = Interoperability by Design

The chargers in this project supported the **Open Charge Point Protocol (OCPP)**, an open standard that governs communication between EV chargers and CMS platforms. The new CMS, EV Connect, is also certified OCPP. Because of this commitment to OCPP by both BTC POWER and EV Connect:

- **No hardware replacemen**t was needed
- Migration relied on **standard commands** instead of proprietary methods
- **Remote reconfiguration** was possible for most chargers
- Troubleshooting was simpler with **well-defined message flows**

In short, OCPP turned a complex transition into a manageable process—and avoided vendor lock-in.

OCPP Helps With:

Task	How OCPP Simplifies
Switching CMS platforms	Standard message protocols reduce custom dev work
Repointing chargers to a new backend	Use ChangeConfiguration or SetNetworkProfile commands
Updating security credentials	Managed through certificate installation and variable settings
Batch migrations	Chargers can be updated in groups with consistent messaging
Fallback mechanisms	Devices can retain last-known good connection settings

Key Results

- **76 chargers successfully migrated** rapidly
- **Uptime preserved** with minimal user impact
- **Process reused** for subsequent L2 charger migrations
- **Reusable toolkit** developed by ChargerHelp for future RaaS and CMS transitions
- **Cross-vendor alignment** with BTC POWER, EV Connect, ChargerHelp and the utility established a template for future collaboration

Best Practices for CMS Migration

Drawing from both this project and our years of experience, here are the top recommendations for a successful transition:

1. Design for Portability: Choose OCPP-Compliant Hardware

> "The ability to migrate charging stations with minimal disruption depends heavily on OCPP compliance."

- **Use certified chargers and CMSs**. Certification ensures interoperability.

- **Avoid vendor lock-in**. Choose the right hardware and software combo for your needs.
- **Standardization saves time and cost** when switching CMSs or scaling your network.

2. Establish a Dedicated Planning Phase

- Allocate **2–4 weeks** for stakeholder alignment before any on-site activity.
- Create a migration pre-requisite checklist to avoid preventable delays around common items like firmware version and OCPP compliance, SIM card transferability or eSIM provisioning, or connectivity tests to the new backend.
- Develop a shared understanding of:
    a. Hardware and firmware readiness
    b. SIM card provisioning
    c. User account/data transfer
    d. Physical signage and QR/NFC update needs

3. Involve All Vendors Upfront

- Include the **hardware OE**M early to confirm firmware compatibility and update paths.
- Align with both the **old and new CMS** teams to validate protocol support.
- For OCPP chargers, confirm:
    a. Firmware supports OCPP 1.6 or 2.0.1
    b. Necessary configuration keys are exposed
    c. Remote commands are accepted and executed correctly

4. Use Remote Configuration Where Possible

OCPP enables remote migration methods, such as:

- SetNetworkProfile (OCPP 2.x)
- ChangeConfiguration (OCPP 1.6)
- InstallCertificate and SetVariablesRequest for secure transitions

Pro Tip: With OCPP 2.0.1, you can pre-load new network settings in a secondary slot (e.g., profile 2), test the connection, and **reset the charger remotely**—reducing site visits, overall project duration and cost.

5. Plan for Edge Cases and Manual Interventions

Even with OCPP, you may encounter:

- Chargers with hard-coded settings (older firmware)
- SIM cards tied to the old CPO's cellular contract
- Configuration keys named differently per manufacturer

Prepare your team with fallback strategies and manual override procedures. For particularly difficult chargers, site visits may still be required.

6. Conduct Controlled Batch Migrations

- Group chargers by model and firmware version
- Migrate in manageable waves during off hours to limit disruption
- Monitor real-time logs for errors or timeouts
- Ensure rollback capability where firmware updates are risky

From Case Study to Industry Standard

This project demonstrated how open standards like OCPP, and the right hardware and CMS partners can ensure seamless and pain free network migrations.

> "This transition project proved that when you combine OCPP-compliant hardware with collaborative project execution and an open software platform like EV Connect, even urgent migrations can be fast, affordable, and scalable."

— ChargerHelp Migration Team

Conclusion: A Framework for the Future

EV networks face inevitable change: new CMS platforms, new vendors, and evolving user expectations. This project—***with EV Connect as the CMS, ChargerHelp as the field execution partner and BTC POWER as the Hardware**—serves as a model for how to execute migrations quickly, securely, and without major disruption.

By aligning around **OCPP**, clear governance, and phased execution, any network can position itself to adapt and scale—without re-inventing the wheel.

APPENDIX D

Successful Migration Case Study: Kople's Transition to the Driivz Platform

Executive Summary

Kople, one of Norway's leading EV charging operators, successfully migrated its charging network and driver base to the **Driivz** platform, powered by the Open Charge Point Protocol (OCPP).

The migration involved:

- **7,000 chargers** from 10 manufacturers (ABB, Alpitronic, Autel, Delta, Efacec, Garo, Kempower, Schneider, Star Charge, Tritium)
- **140,000 driver account**s
- Completed in just **4 months** from planning to go-live

The project demonstrates the **power of OCPP as an open industry standard**, enabling hardware-agnostic migrations, reducing vendor lock-in, and ensuring long-term scalability. Using Driivz's proven migration templates and the special migration tools for data transformation, Kople and Driivz achieved a smooth, disruption-free transition. The result: enhanced operational excellence, seamless driver experience, and a future-proof charging ecosystem aligned with OCA standards.

Migration Scope

Kople's legacy backend provider no longer met the growing demands of scale, interoperability, and open ecosystem integration. To support its expansion and improve service quality, Kople migrated to the Driivz platform.

Scope of migration:

- **Chargers**: 7,000 units across multiple global vendors, highlighting the importance of OCPP's vendor-agnostic approach
- **Drivers**: 140,000 active accounts migrated to ensure continuity of service
- **Timeline**: 4 months from initial planning to final cut-over The project highlights Driivz's ability to support large, multi-vendor chargers at scale — one of the **core strengths of the OCPP standard**.

Migration Process and Outcome

The migration process was executed in phases to ensure continuity and minimize risks:

- **Preparation**: joint planning with Kople, defining data migration and charger connectivity strategy
- **Data Migration**: used Driivz templates and Driivz migration tools to extract, cleanse, transform, and validate charger and driver data
- **Charger Testing**: each manufacturer's model was tested and validated in Driivz's test environment via OCPP

- **Cut-over**: chargers were reconfigured to point to the Driivz backend; routing and VPN changes were coordinated seamlessly

Outcome:

- **Seamless Transition**: no disruption for EV drivers during the migration
- **Future-Proof Platform**: Kople now benefits from open-standards-based scalability and interoperability
- **Enhanced Reliability**: improved charger uptime and operational monitoring with Driivz's 24/7 management tools
- **Customer Experience**: a smoother, more consistent charging experience for 140,000 drivers

This successful project underscores how adopting OCPP with the Driivz platform empowers charging operators like Kople to scale, innovate, and deliver best-in-class EV charging services.