Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií (KIT)

Bakalářská práce

Implementace dobíjecích stanic pro prostředky eMobility do síťové infrastruktury

Jakub Beneš

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jakub Beneš

Systémové inženýrství a informatika
Informatika

Název práce

Implementace dobíjecích stanic pro prostředky eMobility do síťové infrastruktury

Název anglicky

Implementation of Electric Vehicle Charging Stations into network infrastructure

---

Cíle práce

Tématem bakalářské práce je implementace dobíjecí stanice eMobility do sítě pomocí komunikačních protokolů OCPP (Open Charge Point Protocol) vzhledem k rozšiřující se síti dobíjecích míst pro dopravní prostředky eMobility v ČR. Hlavním cílem práce je zhodnotit a doporučit různé možnosti implementace dobíjecích stanic do sítě s kanálem zpětného ovládání a komunikace dobíjecí stanicí

Dílčí cíle:
- analyzovat typy a možnosti připojení dobíjecích stanic,
- charakterizovat problematiku odlišných možností připojení různých výrobců a vzájemné nekompatibility jednotlivých protokolů,
- definovat preference připojení dobíjecí stanice ze strany IT oddělení,
- navrhnout postup implementace dobíjecích stanic s rozdílnou kompatibilitou do sítě.

Metodika

Metodika řešené problematiky bakalářské práce je založena na analýze možností informačních technologií v rámci dobíjecích stanic pro elektromobily. Vlastní zpracování je realizováno na studiu, analýze a vlastních zkušenostech s implementací dobíjecích stanic do síťově infrastruktury.

Návrh možných řešení implementace stanic vychází ze získaných zkušeností a technologických možností jednotlivých dobíjecích stanic. Na základě teoretických a praktických poznatků budou vypracovány možné postupy implementace dobíjecích stanic do síťově infrastruktury vzhledem k možnostem jednotlivých technologií.

Doporučený rozsah práce

30-40 stran

Klíčová slova

dobíjecí stanice, elektromobily, e-mobilita, OCPP, síťová infrastruktura, soap, json

---

Doporučené zdroje informací

Corzato, G. & Secco, Luca & Rasheed, Arslan & Nagar, Atulya & Secco, Emanuele. E-Mobility: smart grid and charging session of electric vehicles [online]. 2018 [cit. 2020-06-10]. Dostupné z: https://www.researchgate.net/publication/323967720_E-Mobility_smart_grid_and_charging_session_of_electric_vehicles

Open Charge Alliance. Open Charge Point Protocol: 1.5 FINAL [online]. 2012-06-08. [cit. 2020-06-10]. Dostupné z: https://www.openchargealliance.org/downloads/

Open Charge Alliance. Open Charge Point Protocol 1.6: 1.6 edition 2 FINAL [online]. 2017-09-28. [cit. 2020-06-10]. Dostupné z: https://www.openchargealliance.org/downloads/

Robert van den Hoed, Robert & Maase, Simone & Helmus, Jurjen & Wolbertus, Rick & Bouhassani, Youssef & Dam, Jan & Tamis, Milan & Jablonska, Bronia. E-mobility: getting smart with data [online]. 2019 [cit. 2020-06-10]. Dostupné z: https://www.researchgate.net/publication/334625203_E-mobility_getting_smart_with_data

WIRGES, Johannes. Planning the Charging Infrastructure for Electric Vehicles in Cities and Regions [online]. 2016 [cit. 2020-06-10]. ISBN 978-3-7315-0501-3. Dostupné z: https://publikationen.bibliothek.kit.edu/1000053253/3877194

Předběžný termín obhajoby

2020/21 LS – PEF

Vedoucí práce

Ing. Michal Stočes, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 20. 7. 2020

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2020

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 13. 03. 2021

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Implementace dobíjecích stanic pro prostředky eMobility do síťové infrastruktury" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14. března 2021 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Michalu Stočesovi, Ph.D. za vedení a podporu této práce. Zároveň bych tímto rád poděkoval kolegům, ze společnosti Pražská energetika, a.s., z oddělení Infrastruktury ICT a oddělení eMobility za umožnění studia a umožnění práce s dobíjecími stanicemi pro elektromobily, které se stávají součástí velké síťové a v současnosti i dopravní infrastruktury.

Implementace dobíjecích stanic pro prostředky eMobility do síťové infrastruktury

Abstrakt

V bakalářské práci se věnuji problematice implementace dobíjecích stanic eMobility do síťové infrastruktury. Stále se jedná o poměrně novou technologii, která je dokončována za chodu a reaguje na aktuální potřeby poskytovatelů dobíjecích míst. Jako každá technologie, trpí i dobíjecí stanice „dětskými bolestmi“. Pokud nastane jakýkoli výpadek nebo nutnost změny konfigurace, je žádost směřována na IT oddělení, které spravuje komunikaci dobíjecí stanice s back-endem. Ze strany IT oddělení je důležité, aby bylo možné dobíjecí stanici spravovat vzdáleně bez nutnosti výjezdu do terénu. V případě, kdy je nutné spravovat několik desítek dobíjecích stanic či více je žádoucí, aby nebyla nutnost fyzické správy dobíjecí stanice. Implementace dobíjecí stanice do sítě je možné řešit několika způsoby. Jedním z nejčastějších způsobů připojení je použití SIM karty s datovým balíčkem. Tento způsob nám nabízí několik možností – pouze přístup k internetu; přístup k internetu v kombinaci s VPN; použití veřejné IP adresy; přístup do vlastního APN.

Klíčová slova: implementace, dobíjecí stanice, IT, eMobilita, back-end, síťová infrastruktura, SIM, VPN, APN, internet

Implementation of Electric Vehicle Charging Stations into network infrastructure

Abstract

This bachelor thesis deals with the problematic of implementing Electric Vehicle Charging Stations into the network infrastructure. EV charging stations are still a relatively new technology, being developed on the go, with manufacturers having to react to the actual needs of the charging point providers. Like any other fast-deployed solution, it also suffers from minor issues. If an outage happens or there is a need to change the configuration of a charging station, all problems and requests are aimed at an IT department. IT department usually maintains communication between the charging stations and the back-end system. A technician is required to be able to configure and control charging stations remotely without the need to service the station in person. This requirement is really important, especially if there are dozens of charging stations to manage. Implementation of EV charging stations into the network infrastructure has many possibilities. One of the most common solutions is the use of a SIM card with a data plan. This solution offers options such as direct access to the Internet, VPN access, using public static IP address or allowing to access to your own APN.

Keywords: implementation, charging station, IT, eMobility, back-end, network infrastructure, SIM, VPN, APN, internet, EV

Obsah

1 Úvod

V bakalářské práci se věnuji problematice implementace dobíjecích stanic eMobility do síťové infrastruktury. Stále se jedná o poměrně novou technologii, která je dokončována za chodu a reaguje na aktuální potřeby poskytovatelů dobíjecích míst. Jako každá nová technologie ve fázi zahajování provozu, trpí i dobíjecí stanice „dětskými bolestmi“.

Pokud nastane jakýkoli výpadek nebo nutnost změny konfigurace, je žádost směřována na IT oddělení, které spravuje komunikaci mezi dobíjecí stanicí a back-endem (systém pro centrální správu a monitorování dobíjecích stanic včetně možností správy zákazníků). Ze strany IT oddělení je důležité, aby bylo možné dobíjecí stanici spravovat vzdáleně bez nutnosti výjezdu do terénu. V případě, kdy je nutné spravovat několik desítek dobíjecích stanic či více je žádoucí, aby nebyla nutnost správy dobíjecí stanice výjezdem technika.

Implementaci dobíjecí stanice do sítě je možné řešit několika způsoby. Jedním z nejčastějších způsobů připojení je použití SIM karty s datovým balíčkem. Tento způsob nabízí několik možností – pouze přístup k internetu; přístup k internetu v kombinaci s VPN; použití veřejné IP adresy; přístup do privátního APN (název přístupového bodu v síti operátora – v ČR například *internet*).

Při použití jakékoli SIM karty s přístupem k internetu je bez problému možné zajistit spojení dobíjecí stanice s back-endem a jejich komunikaci pomocí integrovanému protokolu OCPP (Open Charge Point Protocol – protokol pro komunikaci dobíjecích stanic), ale možnost vzdálené konfigurace má svá úskalí. Část konfigurace je možné do dobíjecí stanice zaslat přes proxy server (OCPP 1.5) nebo tunelovým spojením, které si dobíjecí stanice sama navazuje a udržuje (OCPP 1.6). K velké části nastavení nebo pro provedení diagnostiky je nutné zajistit přístup do integrovaného konfiguračního rozhraní stanice – nejčastěji webové grafické rozhraní. Pokud dojde k rozpojení zmíněného tunelu mezi dobíjecí stanicí a back-endem, není možné jakkoli stanici konfigurovat nebo vzdálený provést restart.

V případě použití SIM s přístupem do internetu v kombinaci s použitím VPN (zkratka pro virtuální privátní síť), dochází k eliminaci nemožnosti vzdálené konfigurace při rozpojení komunikačního tunelu. Dobíjecí stanice je tak připojena k back-endu, ale současně je navázán VPN tunel na hlavní VPN server, který nám vytváří možnost přímého připojení k rozhraní stanice. Software dobíjecí stanice si tak udržuje komunikační tunel s back-endem, který nám při rozpadu neovlivní správcovské možnosti pomocí VPN tunelu.

U některých dobíjecích stanic, které podporují pouze protokol OCPP 1.5, je nutnost použití proxy serveru pro vzdálené ovládání stanice. Avšak některé dobíjecí stanice obsahují bezpečnostní prvek, který kontroluje webovou adresu back-endu a adresu, ze které přichází vzdálený příkaz. Pokud je dobíjecí stanice spojená s back-endem na adrese *https://AdresaBackendu.com:8443*, ale příkaz přichází z adresy *https://AdresaProxy.com*, stanice odmítne reagovat na příchozí příkaz. V tomto případě je nutné použít alternativní metodu připojení – například použít SIM s veřejnou IP adresou, aby mohl back-end se stanicí komunikovat napřímo bez nutnosti potřeby proxy serveru. Tímto způsobem je možné vyřešit problém s ovládáním stanice, ale vystavujeme dobíjecí stanici bezpečnostnímu riziku z důvodu použití veřejně dostupné IP adresy.

Optimálním případem je využití SIM karty s přístupem do vlastního APN. Tento případ je nejlepším řešením za použití SIM zejména pro střední až velké poskytovatele dobíjecích míst. Vyžaduje nutnost zařízení privátního APN u operátora. Tento způsob je schopný zajistit 99,99% dostupnost konfiguračního rozhraní dobíjecí stanice, pokud nenastane výpadek v síti operátora nebo ve firemní infrastruktuře – výpadek u operátora ohrožuje veškeré způsoby připojení pomocí datové SIM karty. Za pomocí této metody je dobíjecí stanice připojena do interní sítě a je dostupná z interní síťové infrastruktury firmy. Pokud dojde z jakékoli příčiny k rozpadu komunikačního tunelu mezi dobíjecí stanicí a back-endem, lze se stále do stanice připojit a provést restart nebo změnu konfigurace.

Nejčastějším problémem u dobíjecích stanic je právě zmiňovaný rozpad tunelu mezi stanicí a back-endem. Pokud dojde k rozpadu, umí na něj některé stanice reagovat opětovným pokusem o navázání spojení, avšak ne všechny stanice obdobnou vlastnost mají,

a i přes opětovný pokus o navázání spojení, se může dobíjecí stanice dostat do režimu chyby a vyžadovat restart pro pokračování.

Pokud stanice ztratí připojení k operátorovi, může dojít k nutnosti výjezdu technika na provedení restartu dobíjecí stanice na místě. V případě ztráty připojení do sítě operátora nebo chyby SIM karty by mohla pomoci implementace technologie IoT LoRa nebo Sigfox. Jedná se o nízkoenergetickou síť, která umožňuje připojení bez nutnosti SIM karty s datovým balíčkem. V případě IoT sítě se nemůže stát, že by došlo například vyčerpání datového limitu SIM karty, nebo nebyla možnost připojení k GPRS/EDGE/LTE síti operátora. Pokud by došlo ke kompletnímu komunikačnímu výpadku stanice, bylo by možné jednou zprávou zaslat řídící elektronice stanice příkaz pro restart a odpadla by nutnost výjezdu technika do terénu.

2 Cíl práce a metodika

2.1 Cíl práce

Tématem bakalářské práce je implementace dobíjecí stanice e-mobility do sítě pomocí protokolů OCPP vzhledem k rozšiřující se síti dobíjecích míst pro dopravní prostředky e-mobility v ČR. Hlavním cílem práce je zhodnotit a doporučit různé možnosti implementace dobíjecích stanic do sítě s kanálem zpětného ovládání a komunikace dobíjecí stanicí**.**

Dílčí cíle

- analyzovat typy a možnosti připojení dobíjecích stanic,
- charakterizovat problematiku odlišných možností připojení různých výrobců a vzájemné nekompatibility jednotlivých protokolů,
- definovat preference připojení dobíjecí stanice ze strany IT oddělení,
- navrhnout postup implementace dobíjecích stanic s rozdílnou kompatibilitou do sítě.

2.2 Metodika

Metodika řešené problematiky bakalářské práce je založena na analýze možností informačních technologií v rámci dobíjecích stanic pro elektromobily. Vlastní zpracování je realizováno na studiu, analýze a vlastních zkušenostech s implementací dobíjecích stanic do síťově infrastruktury.

Návrh možných řešení implementace stanic vychází ze získaných zkušeností a technologických možností jednotlivých dobíjecích stanic. Na základě teoretických a praktických poznatků budou vypracovány možné postupy implementace dobíjecích stanic do síťově infrastruktury vzhledem k možnostem jednotlivých technologií.

3 Teoretická východiska

3.1 Open Charge Point Protocol

Open Charge Point Protocol [1][3][4][8] (zkráceně OCPP) je normovaný, veřejně uznávaný protokol pro komunikaci s dobíjecí stanicí. Open Charge Point Protocol má ve své správě Open Charge Alliance (zkráceně OCA), která se skládá z firem stojícími za vývojem řešení dobíjecích stanic a partnery eMobility.

Aliance se stará o vývoj a podporu protokolů OCPP. V současnosti nejrozšířenějším protokolem je verze OCPP 1.6, která v současnosti vyhovuje většině požadavků partnerů eMobility a poskytovatelům dobíjecích míst [5].

Dříve se používal protokol OCPP 1.5, který je dodnes podporován 99 % dobíjecích stanic – některé dobíjecí stanice nemají v současnosti bohužel ani implementovanou dokonalejší verzi 1.6 a fungují pouze na starém protokolu. Zároveň byl již představen protokol OCPP 2.0, který prozatím neimplementoval téměř žádný producent dobíjecích stanic, protože verze 1.6 je jednoduše dostačující.

3.1.1 OCPP 1.5

Open Charge Point Protocol verze 1.5 [6][9] byl představen již v roce 2009, ale hotový jako celek v používané formě byl uvolněn v červnu 2012 [3]. Dodnes se s ním můžeme setkat i přes chybějící rozšíření verze 1.6. Jedním z výrobců dobíjecích stanic, kteří stále aktivně využívají tento protokol verze 1.5 je výrobce a dodavatel dobíjecích stanic Siemens AG [11]. Protokol OCPP 1.5 využívá SOAP komunikaci pomocí webových protokolů http a https.

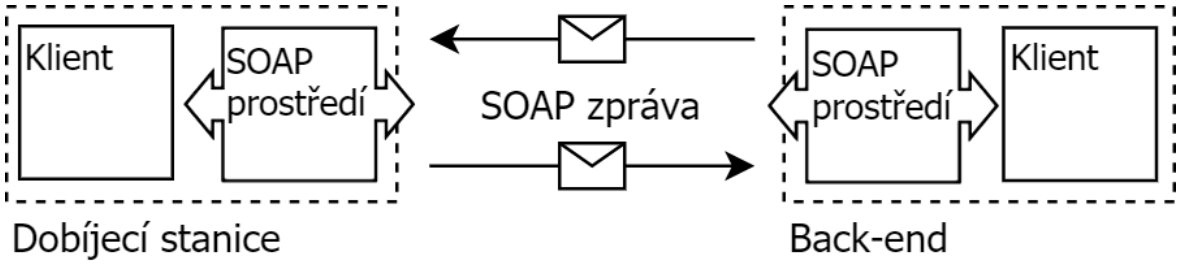
3.1.1.1 SOAP

Jedná se o komunikační *Simple Object Access Protocol*, který využívá jazyk XML pro komunikaci. Díky tomu lze říci, že se jedná se celkem přehledný způsob komunikace mezi dobíječkou a back-endem díky přímé čitelnosti zprávy pro člověka

a jednoduchého zpracování výpočetní technikou. Protokol SOAP je univerzální komunikační způsob, který se skládá ze základních 3 částí – obálky (angl. envelope), hlavičky (angl. header) a zprávy (angl. body) [12]. Přestože se nemusí na první pohled zdát, jedná se celkem o rozsáhlou strukturu, která může vyžadovat více výpočetních prostředků, než by bylo pro komunikaci mezi stanicí a back-endem nutné.

3.1.1.2 Způsob komunikace

Protokol OCPP 1.5 využívá standardizovaný protokol SOAP pro komunikaci mezi dobíjecí stanicí a back-endem, který využívá pro přenos běžný internetový protokol http[1], nebo jeho zabezpečenou verzi https. Jedná se o jednosměrný způsob komunikace, který lze přirovnat ke klasické poštovní komunikaci [12]. Dobíjecí stanice zabalí do obálky zprávu, pošle ji back-endu, který zprávu následně rozbalí a klient její obsah zpracuje (Obrázek 1). Stejným způsobem probíhá i komunikace druhým směrem.



Obrázek 1 — Schéma komunikace pomocí protokolu SOAP, zdroj: autor

3.1.2 OCPP 1.6

Open Charge Point Protocol verze 1.6 [6][10] byl představen o několik let později v roce 2015 [3]. V současnosti se jedná o nejrozšířenější protokol pro komunikaci mezi dobíjecími stanicemi a centrálními systémy. Díky své obsáhlosti vyhovuje již všem potřebám týkajícím se požadované komunikace a správy dobíjecích stanic. Tento protokol

[1] Více informací k protokolu HTTP na webové stánce An overview of HTTP - HTTP | MDN <https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview>

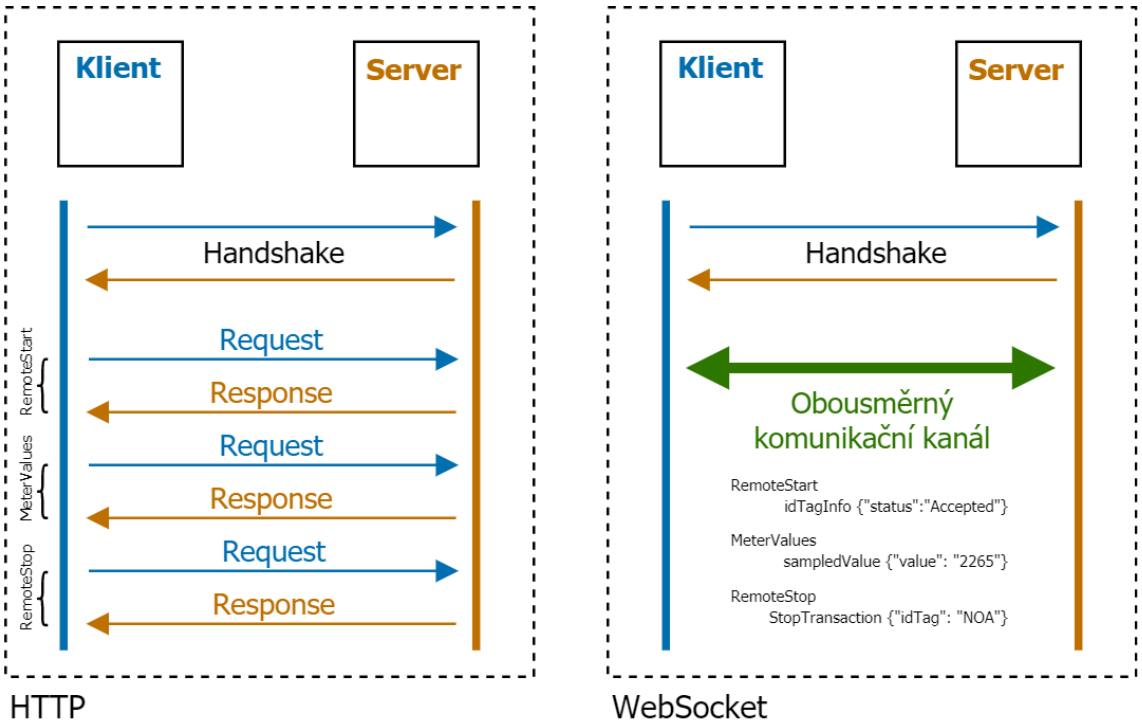
nabízí také možnost využití SOAP pro komunikaci pomocí webových protokolů http a https, ale zároveň přidává možnost JSON komunikace využívající protokolu WebSocket v zabezpečené i nezabezpečené verzi – ws a wss [4][6][8].

3.1.2.1 JSON

S příchodem OCPP 1.6 přišla implementace standardizovaného formátu JSON [13]. Jedná se o formát, který je pro člověka jednoduše čitelný jako tomu bylo v případě OCPP 1.5 a jazyku XML. Ve skutečnosti je možné obecně tvrdit, že JSON je lehčí alternativou XML, protože postrádá značky a atributy i přes zachování veškerých potřebných informací, které jsou nutné pro komunikaci. JSON je tak ideální volbou pro výměnu dat při zachování malého objemu přenesených dat. Díky své minimalistické formě není tolik náročný na zpracování a přenos jako je tomu v případě protokolu SOAP s využitím XML.

3.1.2.2 Způsob komunikace

V případě komunikace pomocí JSON je pro přenos využíván protokol WebSocket. WebSocket je obousměrný, full-duplexní protokol využívající jedno samostatné TCP spojení [14]. Oproti jednosměrnému protokolu http, umožňuje obousměrné spojení lepší přenos informací v reálném čase. Pro komunikaci je možné využívat URI ws, nebo wss pro zabezpečené spojení. V praxi dochází, oproti http, k navázání spojení pomocí handshaku a následnému otevření trvalého spojení mezí klientem (dobíjecí stanice) a serverem (back-end) viz *Obrázek 2*.



Obrázek 2 — Porovnání způsobu komunikace pomocí protokolů HTTP a WebSocket, zdroj: autor

3.1.3 Porovnání protokolu OCPP 1.5 a OCPP 1.6

Oba zmíněné protokoly umožňují to nejdůležitější – komunikaci dobíjecí stanice s back-endem ve správě poskytovatele dobíjecích míst. Avšak je samozřejmostí, že každá novější verze odstraňuje nedostatky a doplňuje žádané funkce dané potřebami nasazení v reálném světě. Komunikace pomocí JSON ve verzi 1.6 přinesla několik výhod jako je jednodušší komunikace back-endu se stanicí, vzdálené ovládání a odpadla nutnost potřeby řešení pro zpětnou komunikaci za pomoci proxy serveru mezi back-endem a dobíjecí stanicí. Jednoznačně lze bez nadsázky podotknout, že protokol OCPP 1.6 je obecně řečeno lepší pro nasazení nových dobíjecích stanic a jejich správu oproti verzi OCPP 1.5. *Další podrobnosti k protokolům OCPP 1.5 a OCPP 1.6 v oficiální dokumentaci spolku Open Charge Alliance [9][10].*

3.2 Back-end

Back-end je aplikační řešení pro správu a monitorování stavu dobíjecích stanic poskytovatelem dobíjecích míst. Těmto centrálním systémům, sloužícím pro správu stanic

se také říká ve zkratce CPO systém neboli Charge Point Operator systém [15]. V závislosti potřeb a požadavků ze strany poskytovatelů služeb v oblasti dobíjení elektromobilů jsou tyto interní systémy vyvíjeny odlišně. Nesetkáme se tedy nikdy s jedním univerzálním systémem, protože každý vývojář má snahu zaujmout svého zákazníka pomocí nadstandardních funkcí, které integruje nebo upravuje na přání zákazníka.

Postupem času se CPO systémy vyvíjeli pro jednodušší a efektivnější správu stanic. Základní funkce pro správu dobíjecích stanic jsou ve většině případů stejné a systémy se převážně liší v grafickém prostředí, možnostech správy zákazníků a vyúčtování. Časem také přibyly administrátorské role, které slouží k umožnění přístupu jednotlivých správců do vlastních sekcí – například správce dobíjecích stanice nemusí mít přístup ke správě zákazníků. Nejdůležitějšími funkcemi těchto systémů je samotná správa dobíjecích stanic – evidence dobíjecích stanic, vzdálená konfigurace, vzdálené ovládání –, správa zákazníků a správa autorizačních médií (NFC karty a čipy) [15].

3.2.1 Komunikace s dobíjecí stanicí

Komunikace mezi dobíjecí stanicí a back-endem je vždy navazována ze strany dobíjecí stanice [7]. Technologicky by ani nebylo ve většině případů možné, aby centrální systém navazoval spojení jako první směrem k dobíjecí stanici. Komunikace mezi back-endem a dobíjecí stanicí využívá protokol OCPP. Zpráva obsahuje jedinečný identifikátor stanice, díky kterému back-end rozezná, o kterou konkrétní dobíjecí stanici se jedná [2][3].

Po úspěšném startu ovládacího systému v dobíjecí stanici je stanicí odeslána stavová zpráva *BootNotification*, která obsahuje základní informace o stanici – výrobce, model stanice, identifikační číslo, sériové číslo, verze firmware, imsi a iccid. Jako další v pořadí jsou následně zaslané zprávy *StatusNotification*, které obsahují informace o dostupnosti dobíjecích bodů neboli konektorů – na základě těchto notifikací upravuje back-end informace o dostupnosti dobíjecí stanice a jejich konektorů[2]. Pokud back-end neobdrží *BootNotification*, je pro něj dobíjecí stanice neviditelná – ze zjednodušeného pohledu *BootNotification* slouží jako potvrzení o úspěšném navázání komunikace mezi stanicí

[2] Dle informací technické podpory CPO systému CharVIS od rakouské společnosti Smatrics.

a centrálním systémem. Pokud systém neobdrží informace o dostupnosti dobíjecích bodů, zobrazí tyto dobíjecí body jako nedostupné.

Komunikace dobíjecí stanice s back-endem probíhá jednoduše řečeno pomocí textových zpráv. Na každou zprávu odeslanou směrem k dobíjecí stanici, stanice zprávu zpracuje a odpoví zpět *Accepted* (přijato), nebo *Rejected* (odmítnuto) [9][10]. V případě *Accepted* se zachová podle příkazu, který byl na stanici odeslán, v případě *Rejected* odmítne povel vykonat. Pokud dojde k odmítnutí pokynu, stanice neposkytuje zpět informaci, z jakého důvodu k odmítnutí došlo – pokud se jedná o nestandardní chování, je na technologickém týmu správy dobíjecích stanic, aby zajistil podchycení tohoto problému a navrhl možné řešení.

3.2.2 Vzdálené ovládání dobíjecí stanice

Dobíjecí stanice připojené pomocí protokolu OCPP 1.6 JSON umožňují přímé ovládání zahájení a ukončení dobíjení, odemknutí, aktivaci a deaktivaci konektoru [10]. Jedná se o základní příkazy, které musí být každý centrální systém schopný odeslat směrem k dobíjecí stanici. Vzdálené ovládání je užitečné zejména při řešení problému s autorizací zákazníka na místě dobíjecí stanice nebo pro implementaci do dalších systémů – například webová nebo mobilní aplikace pro dobíjení[3], platební brána pro neregistrované zákazníky apod.

Dle protokolu OCPP musí každá stanice podporovat *RemoteStart* a *RemoteStop* pro vzdálené zahájení a ukončení nabíjení [9][10]. V praxi to znamená, pokud má zákazník problém s autorizací pomocí vlastní čipové karty, připojí na místě elektromobil k dobíjecí stanici, kontaktuje zákaznickou linku poskytovatele dobíjecích míst a vzdáleně je ze strany zákaznické podpory možné zaslat stanici pokyn, aby pro zahájení dobíjení. Dalším příkazem je *UnlockConnector*, který slouží k odemknutí konektoru, pokud dojde ze strany dobíjecí stanice v případě chyby k jeho blokaci anebo neodemčení z dalších příčiny (například chyba na připojeném vozidle). Posledním základními příkazy je *ActivateConnector* a *DeactivateConnector*. Tyto příkazy slouží pro povolení nebo blokaci

[3] Dle informací technické podpory provozovatele dobíjecích míst Smatrics

nabíjecího konektoru na stanici. Například v případě fyzické chyby na interních komponentech dobíjecí stanice, je možné jednotlivý konektor blokovat, aby z něj nebylo možné dobíjet – ze strany dobíjecí stanice dojde nejčastěji k signalizaci červeným podsvícením o nedostupnosti konektoru.

3.2.3 Vzdálená správa dobíjecí stanice

Pro vzdálenou správu dobíjecí stanice se používají zejména čtyři nejdůležitější příkazy – *GetConfiguration*, *ChangeConfiguration*, Soft reset a Hard reset. Příkaz G*etConfiguration* slouží k výpisu nastavení dobíjecí stanice. Po vypsání nastavení je možná manuální editace a po uložení je příkazem z back-endu odeslána zpět do dobíjecí stanice, která si nové nastavení aplikuje. V případě nekompatibilního nastavení reaguje stanice zprávou *Rejected*, zachová se původní nastavení a nová konfigurace se ignoruje [10].

Příkazy pro reset slouží pro restartování stanice. Dělí se na soft a hard reset. Soft reset restartuje pouze komponenty ovládacího systému dobíjecí stanice (operační systém) a samostatné procesy jako jsou webový server, správa síťového připojení apod. Ostatní elektronika zůstane v původním stavu. Hard reset funguje obdobně jako u osobních počítačů – provede restart kompletně celého systému včetně hardware komponent.

3.3 Možnosti připojení dobíjecí stanice do sítě

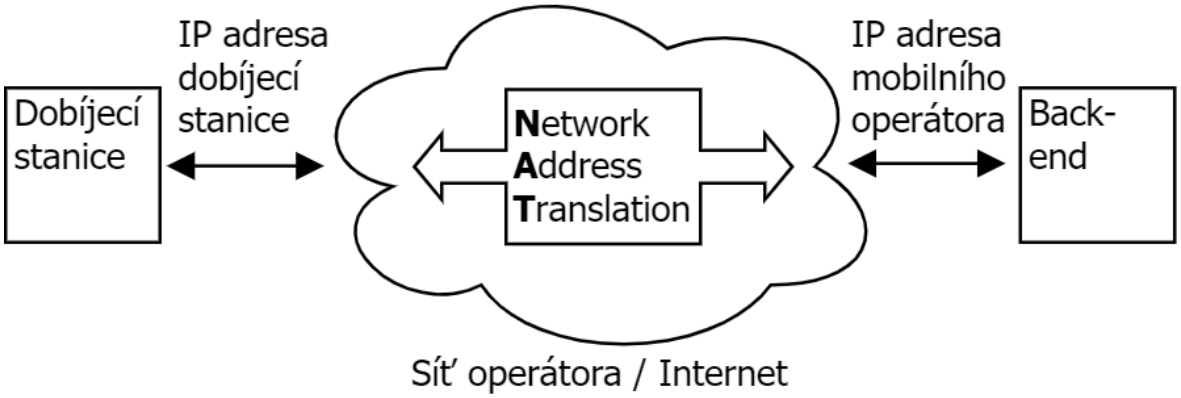
Možnosti připojení dobíjecí stanice do sítě se odvíjí zejména podle jednotlivých výrobců dobíjecích stanic. Obecně ale platí, že všechny stanice umožňují připojení pomocí datové SIM karty mobilního operátora [2].

3.3.1 Připojení pomocí SIM karty

3.3.1.1 SIM karta s přístupem do veřejného internetu

Jednou z nejčastějších variant je běžnější datová SIM karta, která je velmi často využívána v přenosných modemech nebo jako SIM určené pro datové připojení tabletů

a notebooků [16]. Datová SIM se připojí do veřejné sítě internet pomocí APN operátora (např. *internet.t-mobile.cz*, ale možné použít i univerzální zkrácený zápis pro všechny operátory V ČR názvem *internet*). Výhodou datové SIM jsou relativně nízké náklady, protože pro běžnou funkčnost dobíjecí stanice stačí, i s rezervou, pouze 100 MB dat na každý měsíc.



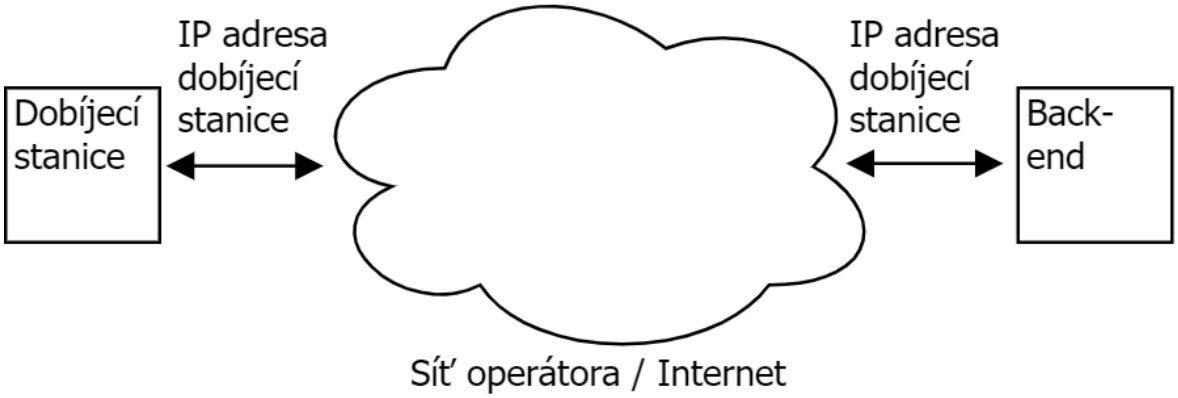
Obrázek 3 — Zjednodušené schéma připojení pomocí SIM karty, zdroj: autor

Teoretickou nevýhodou tohoto řešení je nedostupnost přímé možnosti konfigurace dobíjecí stanice pomocí jejího integrovaného konfiguračního rozraní. V případě použití APN operátora je stanice ukryta za NAT překladovými servery a není tedy možné se na ni přímo připojit i pokud známe její IP adresu (Obrázek 3).

3.3.1.2 SIM karta s veřejnou IP adresou

Další způsobem připojení dobíjecí stanice je využití SIM karty s veřejnou IP adresou. Toto řešení vyžadují některé dobíjecí stanice pro správnou funkčnost. Jedná se o připojení do sítě, kdy má SIM karta svoji pevně přidělenou IP adresu, která je přímo vystavena do sítě internet [16]. Tento způsob je velmi podobný řešení pomocí přístupu přes veřejný internet, jen s výhodou, možnosti přímého přístupu ke konfiguračnímu rozhraní stanice díky odkryté, veřejně dostupné IP adrese ze sítě internet.

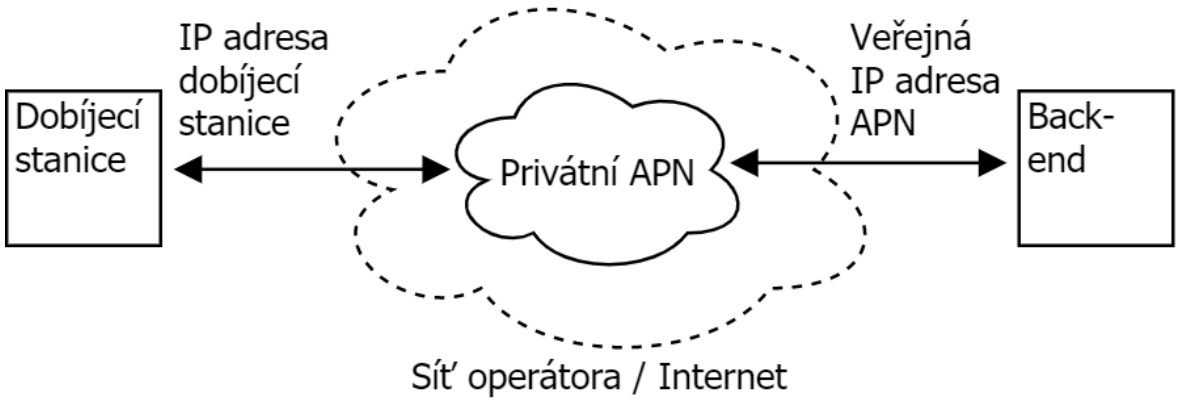
Na místě je také zmínit nevýhodu možnosti útoku na dobíjecí stanici – IP adresa je veřejná, a každý kdo bude znát tuto adresu se na ni může pokusit připojit. Požadavkem je následně nutnost kvalitního zabezpečení dobíjecí stanice, aby bylo možné předejít neoprávněnému přístupu.



Obrázek 4 — Zjednodušené schéma připojení pomocí veřejné IP adresy, zdroj: autor

3.3.1.3 SIM karta s přístupem do vlastního APN

Třetí možností řešení přístupu je konektivita pomocí SIM karty s přístupem do privátního APN pomocí sítě operátora. Řešení připojením vlastního APN je velmi efektivním způsobem, protože SIM karta je připojena k interní síti a je možné se k ní napřímo připojit [16]. Velkou nevýhodou je finanční náročnost tohoto řešení – napojení interní sítě na APN pomocí operátora a poplatek za zřízení, konfiguraci dle vlastních požadavků a správu operátorem. Jedná se přesto o velmi vhodnou možnost připojení v případě středních a velkých firem s větším počtem dobíjecích stanic. Varianta využití privátního APN se také jeví jako jedna z bezpečných možností připojení dobíjecí stanice do sítě, protože stanice není přístupná z veřejné sítě jako je tomu u použití veřejné IP adresy [17].



Obrázek 5 — Zjednodušené schéma připojení pomocí privátního APN, zdroj: autor

3.3.2 Připojení pomocí externího zařízení, LAN

Mimo přímého použití datových SIM karet v elektronice dobíjecí stanice je také možné využití dalších způsobů připojení jako jsou externí USB modemy nebo připojení pomocí LAN a externího routeru. Možnosti těchto technologií se liší každým jednotlivým výrobcem a modelem dobíjecí stanice. Některé dobíjecí stanice pak umožňují výběr z několika variant možností připojení bez dalších složitějších úprav a nastavení.

3.3.3 Budoucnost IoT sítí – LoRa a Sigfox

Vzhledem k možným problémům ohledně dostupnosti kvalitního pokrytí mobilním signálem sítě operátora, je vhodné také uvažovat o dalších možnostech a způsobech připojení dobíjecí stanice do sítě. Jednou z možností je nízkoenergetická síť pro zařízení IoT (Internet of Things) v Evropě známá jako LoRa nebo Sigfox [18][19]. Jedná se o sítě, které mají lepší pokrytí než běžné 2G/3G nebo LTE sítě operátorů při nižší energetické náročnosti.

V současnosti se tyto sítě využívají pouze pro jednosměrnou komunikaci od klienta směrem k serveru. Problémem této sítě, že neobsahují při současné jednosměrné komunikaci nedisponují možností kontroly, jestli došlo k úspěšnému doručení informace od klienta na server či nikoli. Pokud by došlo k výpadku konektivity nebo ke změnám v intenzitě pokrytí signálem, klient by odesílal zprávy směrem k serveru a považoval by je automaticky

jako doručené[4]. V současném stavu, pokud nemá dobíjecí stanice odpověď od serveru (nepodaří se odeslat zprávu), je zařazena do fronty na opětovné odeslání a stanice se neustále pokouší o odeslání informace směrem k back-endu.

V síti LoRa a Sigfox je obousměrná komunikace možná, ale její implementace je složitější. Po odeslání zprávy by tak muselo docházet k odeslání potvrzující zprávy o příjmu informace. Na druhou stranu se však jedná o cenově výhodné připojení, protože se platí pouze za každou přenesenou zprávu. V praxi by tak bylo možné použití například pro zaslání příkazu pro restart dobíjecí stanice v případku výpadku sítě u mobilního operátora.

[4] Dle zkušeností se spolehlivostí GPS sledovacího zařízení Invoxia používajícím připojení k nízkoenergetické síti Sigox, https://www.invoxia.com/cz/gps-tracker

4 Vlastní práce

Veškeré testy, sběr dat a výsledné závěry se zakládají na testování a práci s dobíjecími stanicemi ABL eMH3 a eMC2, Alpitronic HYC, Ensto EVB a EVF, Voltdrive Silentium a Silentium P a v neposlední řadě Kostad/Siemens Triberium podporující pouze OCPP 1.5. Ověření konfigurace a dobíjení probíhalo pomocí vozidla Peugeot iON 2011 a testovacího měřidla Metrel A 1532.

4.1 Napojení dobíjecí stanice k back-endu

Základní způsob napojení dobíjecí stanice se liší podle použitého protokolu OCPP. Protokol OCPP 1.5 pro napojení stanice a možnost vzdáleného ovládání vyžaduje prostředníka ve formě proxy serveru, který zajišťuje komunikaci ze strany back-endu směrem k dobíjecí stanici.

V případě použití novějšího protokolu OCPP 1.6 není nutnost použití proxy serveru a komunikaci si dobíjecí stanice navazuje a udržuje s centrálním serverem sama. Je tomu tak z důvodu formy komunikace vysvětlené v sekci *3.1 Open Charge Point Protocol*. K rozšířenému popisu možností připojení bez ohledu na verzi použitého protokolu více informací v sekci *4.2 Způsoby integrace dobíjecí stanice do sítě.*

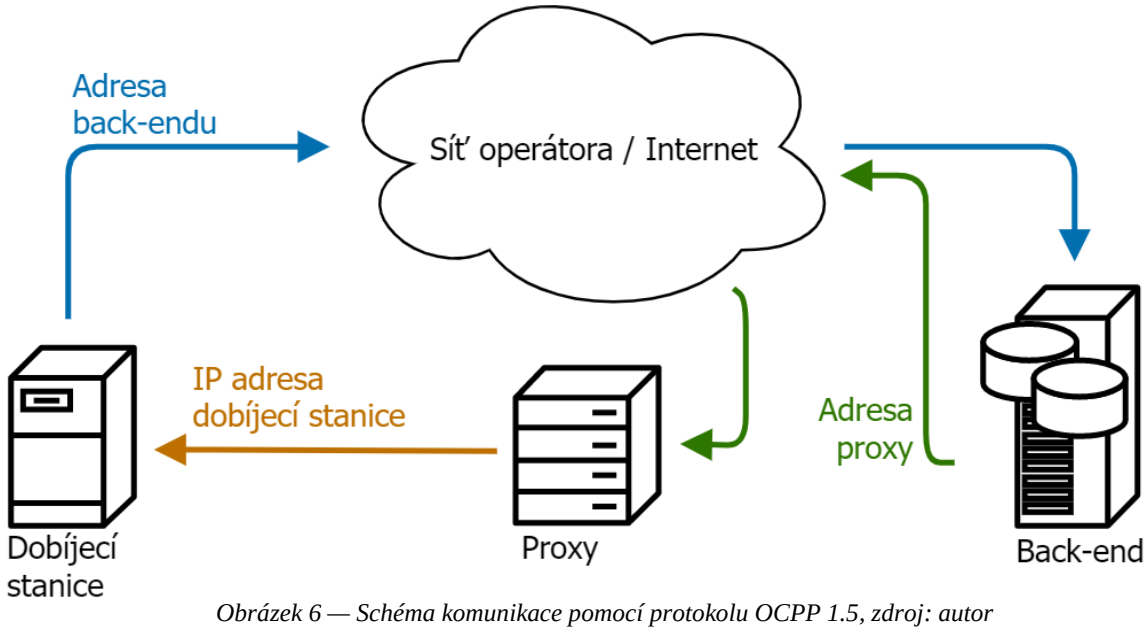
Základní parametry nutné pro připojení dobíjecí stanice k back-endu obsahují jedinečný identifikátor stanice, zvolený způsob komunikace, adresu back-endu a v případě OCPP 1.5 i adresu a port na straně dobíjecí stanice pro vzdálené ovládání. Pomocí unikátního volitelného identifikátoru stanice (zkráceně ID), rozeznává back-end o kterou konkrétní stanici se jedná. Adresa back-endu určuje jakým způsobem se stanice k serveru připojí a kde je server v síti umístěn. U verze OCPP 1.5 adresa stanice pro zpětné ovládání popisuje, kde je v síti stanice umístěna, aby s ní mohl centrální server navázat spojení a komunikovat.

4.1.1 OCPP 1.5

Při zvolení staršího protokolu OCPP 1.5 je zapotřebí brát v úvahu proxy server umístěný mezi back-endem a dobíjecí stanicí. Komunikace probíhá následně tímto způsobem: stanice zahájí inicializaci připojení k back-endu napřímo, v back-endu dojde k nastavení (ručně nebo automaticky) adresy pro zpětné ovládání a server vrátí odpověď proxy serveru, který na základě identifikátoru stanice předá zprávu odpovídající dobíjecí stanici.

Proxy server plní velmi důležitou funkci prostředníka. Z pravidla musí obsahovat seznam dobíjecích stanic s jejich IP a URL adresami pro vzdálené ovládání, na základě, kterého předává zprávy jednotlivým stanicím. Může se jednat o jednoduchou webovou aplikaci běžící například na webovém aplikačním frameworku Django, která má přístup k databázi stanic.

Veškerá komunikace z back-endu směrem ke stanici je směrována přes tento proxy server, který na základě identifikačního jména dobíjecí stanice, obsaženého v každé příchozí zprávě, rozhodne a zprávu nasměruje k odpovídající stanici. Proxy server nemusí sloužit pouze k jednosměrné komunikaci, ale díky své jednoduchosti je také možné odesílat touto cestou zprávy od dobíjecí stanice směrem k back-endu. Vlastnost možnosti obousměrné komunikace pak umožňuje další práci se stavovými zprávami, které stanice posílají, protože je možné je částečně modifikovat dle vlastních potřeb a požadavků.



Obrázek 6 — Schéma komunikace pomocí protokolu OCPP 1.5, zdroj: autor

Stanice směrem k serveru komunikuje napřímo, ale komunikace směrem od back-endu ke stanici probíhá přes prostředníka, kterým je proxy server (Obrázek 6). Jedná se o celkem snadné a funkční řešení, které ale nemusí být kompatibilní se všemi dobíjecími stanicemi.

Z toho vyplývá, že je nutné vést na straně proxy serveru aktuální záznamy obsahující aktivní dobíjecí stanice s přiřazením jejich identifikátorů, IP adres a portů pro komunikaci. Jakmile by na serveru byl seznam neaktuální anebo obsahoval chybu, nedojde k přesměrování komunikace ke stanici a nebude ji tak možné vzdáleně ovládat.

Například rychlou dobíjecí stanici Triberium od společnosti Siemens/Kostad není možné používat s proxy serverem, protože stanice kontroluje adresu serveru, se kterou napřímo komunikuje a proti této adrese porovnává adresu proxy serveru, který komunikuje směrem ke stanici. Při testech v praxi tedy nebylo možné použít tento způsob připojení, protože adresy navzájem neodpovídaly – adresa back-endu *https://AdresaBackendu.com* nebyla identická s adresou proxy *https://AdresaProxy.cz*. Adresa back-endu byla externí adresa, která byla rozdílná oproti interní adrese proxy serveru. Jediným možným řešením bylo použití SIM karty s veřejnou IP adresou.

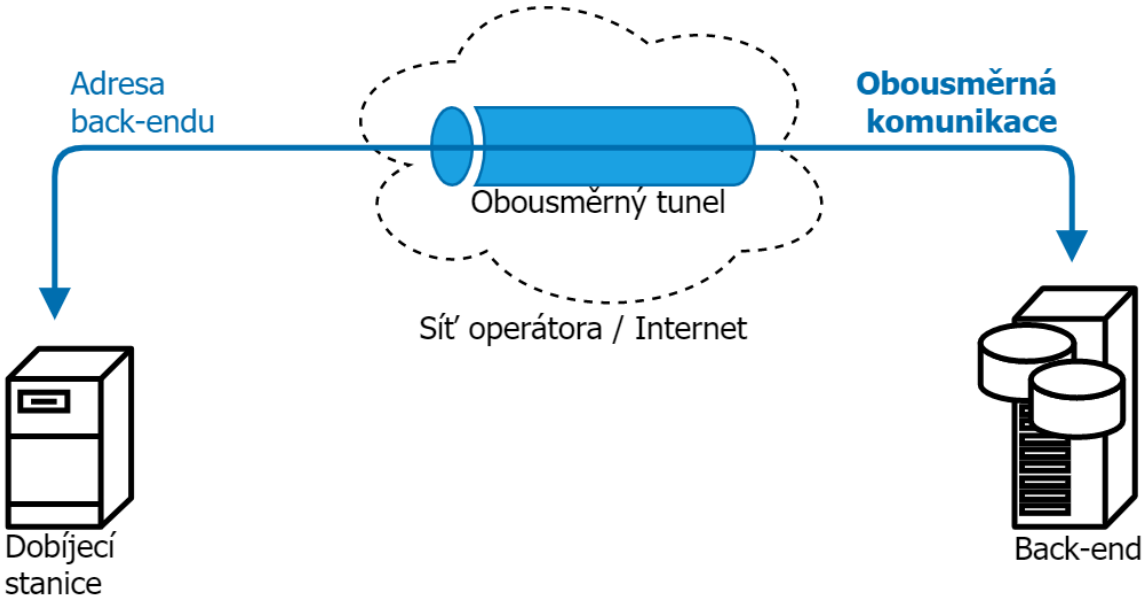
4.1.2 OCPP 1.6

V případě použití mladšího protokolu OCPP 1.6, díky využití WebSocket spojení, opadá nutnost využívání proxy serveru, protože stanice si sama udržuje se serverem obousměrný pomyslný tunel, díky kterému spolu komunikují (Obrázek 7). Díky změnám ve způsobu komunikace právě mezi verzemi 1.5 a 1.6 se jedná o nejjednodušší možný způsob komunikace, který nelimituje správce při zvolení jakéhokoli způsobu integrace dobíjecí stanice do sítě. Většina stanic podporuje již tento protokol (OCPP 1.6) a není tedy nutnost využívat starší verzi 1.5, která nemusí být již v některých stanicích implementována.

4.2 Způsoby integrace dobíjecí stanice do sítě

Nejčastější možností integrace do síťové je využívání síťové konektivity pomocí datové SIM karty, která se umisťuje přímo do integrovaného modemu v dobíjecí stanici. V případě, že není možné použít připojení pomocí sítě mobilního operátora, je nutné přizpůsobit se aktuálnímu místu instalace stanice a volit dostupné alternativní možnosti navázání konektivity či lokální poskytovatele internetového připojení.

Možnosti integrace se odvíjí od vlastních možností způsobů připojení dobíjecích stanic. Každý výrobce používá své vlastní standardy a metody možností připojení. Způsob připojení se dále odvíjí od požadavků na náklady spojené s provozováním stanic, možnosti údržby a konfigurace, nebo dle geografického rozmístění dobíjecích stanic pro prostředky eMobility.



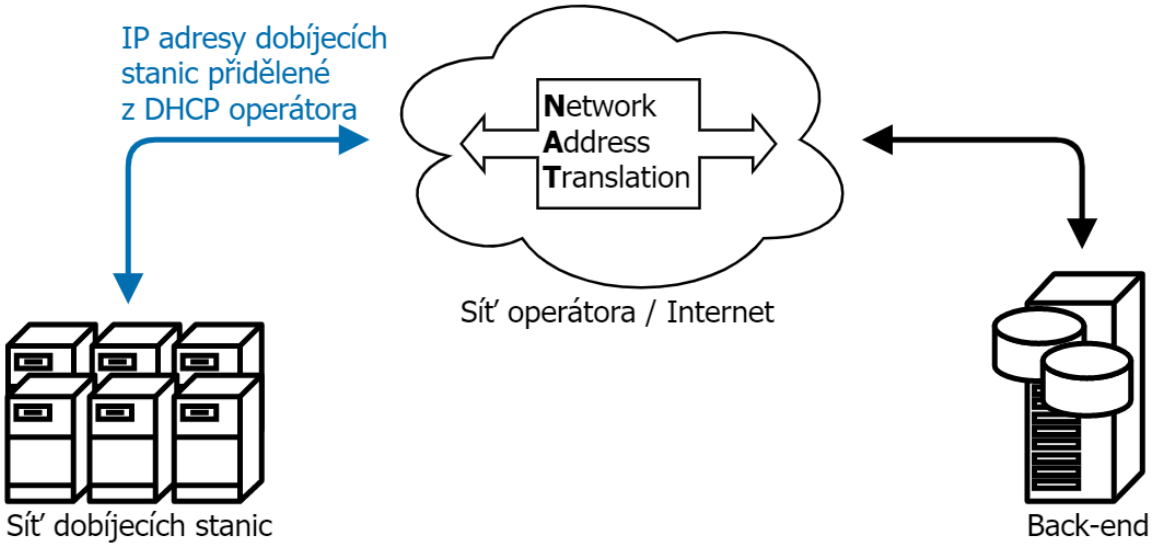
Obrázek 7— Schéma komunikace pomocí protokolu OCPP 1.6, zdroj: autor

4.2.1 Připojení pomocí SIM s přístupem do internetu

Základním připojením je využití datové SIM karty s přístupem do veřejného internetu pomocí sítě operátora. Dobíjecím stanicím běžně stačí balíček obsahující 100 MB dat / měsíc. Připojení touto metodou je nejlevnějším z možných řešení konektivity s centrálním systémem pro správu stanic. Způsob připojení pomocí veřejného internetu je vhodný

pro všechny typy stanic, které disponují integrovaným 2G/3G/LTE modemem – 99 % stanic má možnost připojení právě pomocí mobilního připojení.

Připojení datovou SIM kartou s veřejným internetem je vhodné pro správu malého počtu stanic v řádu jednotek až pár desítek kusů. Pokud by se jednalo o větší množství, je vodné, aby byly dobíjecí stanice umístěny geograficky blízko sebe v menší lokalitě – například v rámci jednoho města. Připojení nelze doporučit pro velké projekty z důvodu



Obrázek 8 — Zjednodušené schéma připojení pomocí veřejného internetu, zdroj: autor

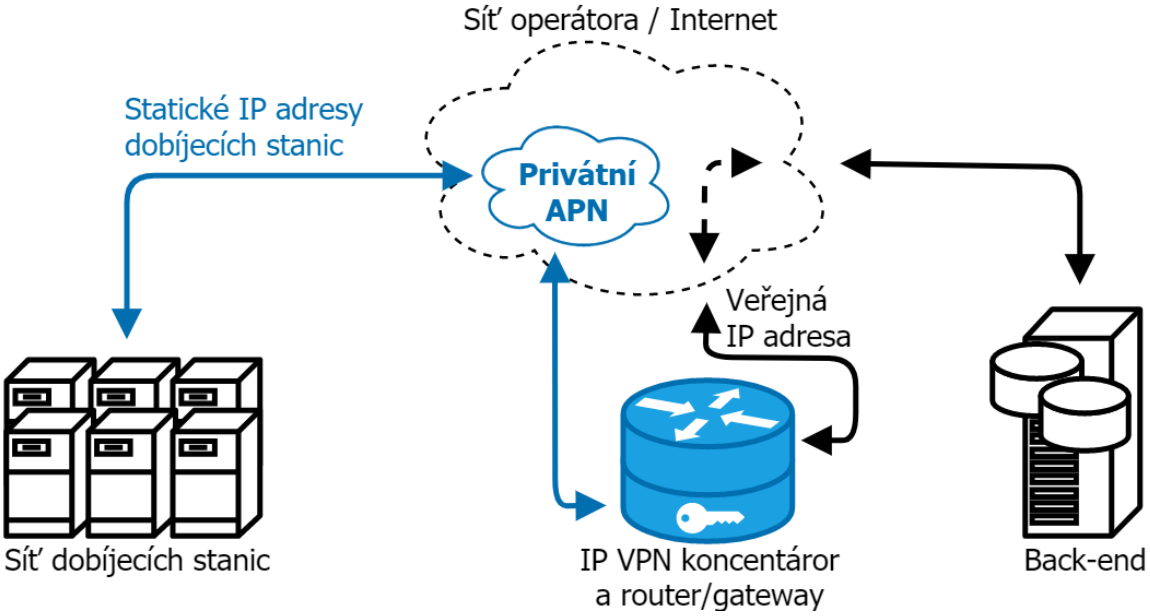
absence pevné koncové IP adresy, a tedy i možnosti připojení se přímo ke stanici a umožnění její správy pomocí integrovaného konfiguračního rozhraní. Každá větší úprava konfigurace stanice vyžaduje výjezd technika na místo, protože možnosti vzdálené konfigurace ze strany back-endu je omezená. Pro základní integraci, správu a monitoring menšího počtu stanic je tato metoda připojení velice vhodná díky technologické a finanční nenáročnosti, i za cenu nutnosti výjezdu technika správy dobíjecích stranic do místa stanice v případě požadavku na rozsáhlejší úpravu konfigurace anebo v případě řešení diagnostiky.

4.2.2 Připojení pomocí SIM s privátním APN

Pro využívání vlastního neboli privátního přístupového bodu (zkr. APN) je nutné zařízení poskytování této služby u operátora mobilních služeb. Cena se odvíjí dle dohody mezi zákazníkem (firmou) a operátorem. Odvíjí se podle rozsahu poskytované služby, komplexností konfigurace sítě a smutné správy ze strany mobilního operátora. Jedná

se o finančně nejnákladnější způsob připojení z důvodu pronájmu vyhrazeného prostoru v síti operátora dle vlastních požadavků. SIM karta má od operátora přiřazenou pevnou IP adresu z rozsahu, který si zákazník s operátorem určí při zřizování APN.

Privátní APN je velmi bezpečný způsob zajištění konektivity a možnosti komunikace mezi dobíjecí stanicí a back-endem, protože SIM karty s přístupem do tohoto APN umožňují komunikaci pouze s interní firemní sítí bez přístupu k internetu (závisí na požadavcích při budování infrastruktury u operátora). Zároveň spojení se síťovou infrastrukturou umožňuje přímý přístup k administrativnímu rozhraní dobíjecí stanice bez nutnosti vystavit dobíjecí stanici do veřejně přístupné části internetu, nebo požadavku na použití prostředníka ve formě proxy serveru.



Obrázek 9— Zjednodušené schéma připojení pomocí privátního APN, zdroj: autor

Velmi zjednodušeně se jedná o vlastní malou síť v celé síti operátora (Obrázek 9), která je plně soukromá a definovaná podle vlastních požadavků. Mimo finanční náročnost, další nevýhodou je závislost na správci sítí ze strany operátora, kteří provádějí požadované změny v síti. Některé úpravy mohou trvat i v rámci týdnů. Správa privátního APN zůstává v rukou operátora a při jakékoli menší změně – například při změně adresy DNS serveru nebo změn v konfiguraci routování, je nutné zadat požadavek technikům operátora, kteří žádané změny v rámci dnů až týdnů aplikují. Řešení komunikace pomocí vlastního APN se hodí spíše pro správu středního až většího počtu stanic v řádu od desítek kusů.

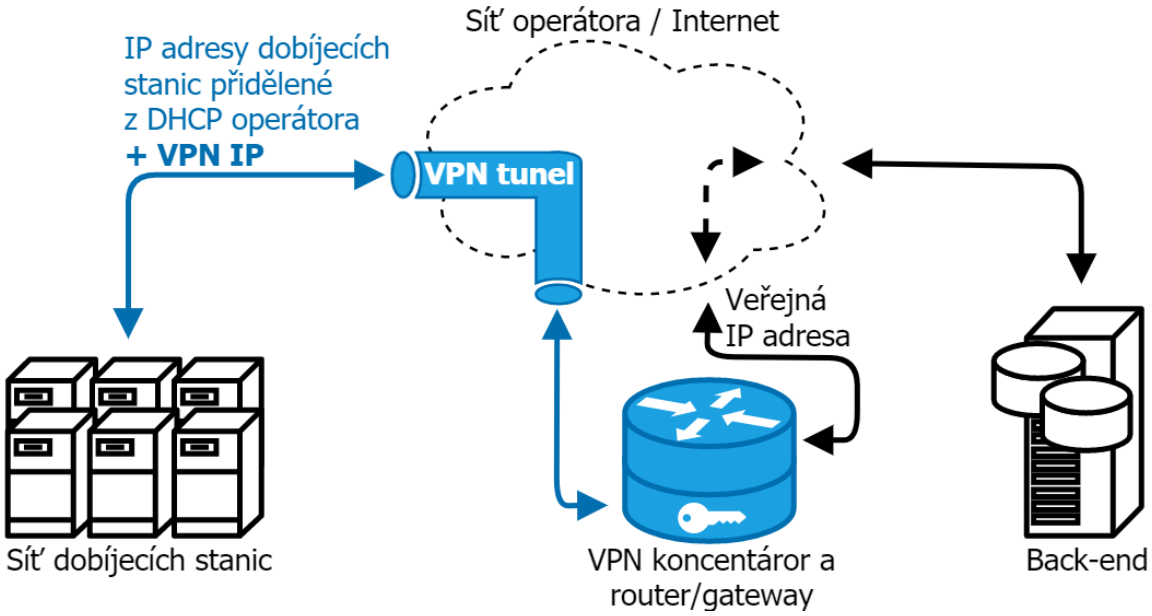
Díky zachování jednoduchého principu připojení je snadná i konfigurace v dobíjecí stanici, kdy se zamění pouze název výchozího APN pro připojení do sítě. V České republice se používá veřejné APN s názvem *internet,* které funguje u všech českých operátorů. Při změně APN dojde po přihlášení SIM karty do sítě operátora k registraci a díky změněnému názvu přístupového bodu (APN) dojde k přidělení předem určené IP adresy a výchozích cest pro komunikaci soukromou sítí v síti operátora.

Výhodou je kompatibilita tohoto typu připojení s 99 % dobíjecích stanic. Ve skutečnosti se na straně stanice jedná o úplně běžný typ připojení SIM kartou s přístupem do sítě operátora, který nevyžaduje další implementované funkce. Nastavení v dobíjecí stanici je téměř identické jako při použití SIM karty s přístupem do veřejného internetu, jen s rozdílem ve způsobu samotné realizace sítě.

4.2.3 Připojení pomocí SIM a VPN tunelu

Připojení za použití VPN tunelu vyžaduje standardní SIM kartu s aktivním datovým balíčkem a připojením k veřejnému internetu. Použití VPN nabízí hned několik možných řešení – PPTP, IPSec a IKEv2 [5]. Jedná se o technologii klient-server. Dobíjecí stanice má roli klienta, který navazuje spojení se serverem umístěným ve firemní síti. VPN spojení funguje na principu vytvoření soukromého tunelu internetem, který umožňuje přímou komunikaci se stanicí i pokud nemá pevně přidělenou IP adresu (Obrázek 10).

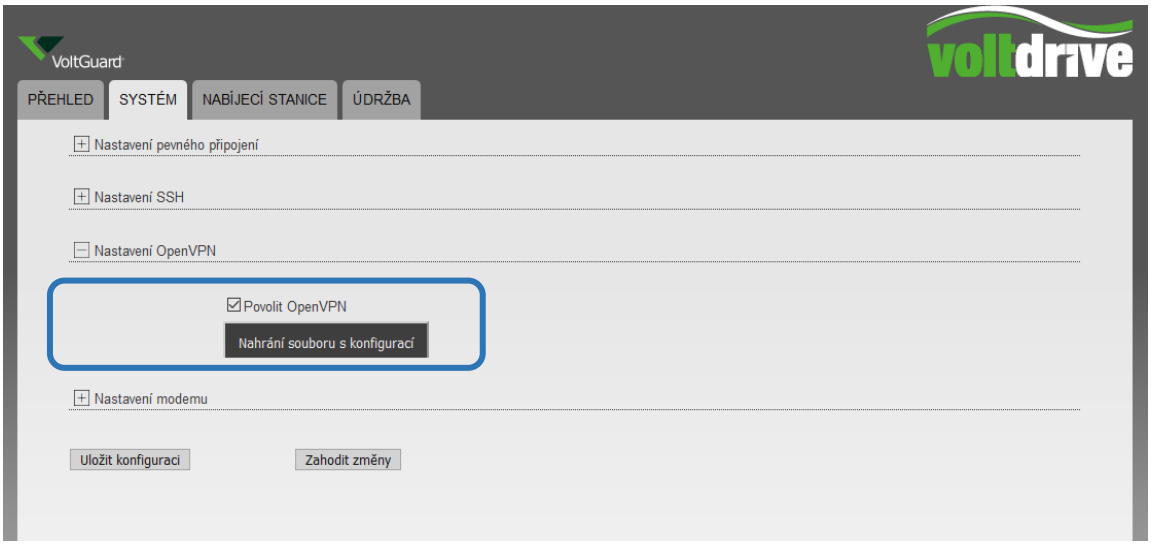
[5] Více informací k VPN připojení: What Is A VPN? | Everything You Need To Know For 2021 | OpenVPN, https://openvpn.net/what-is-a-vpn/



Obrázek 10— Zjednodušené schéma připojení pomocí VPN tunelu, zdroj: autor

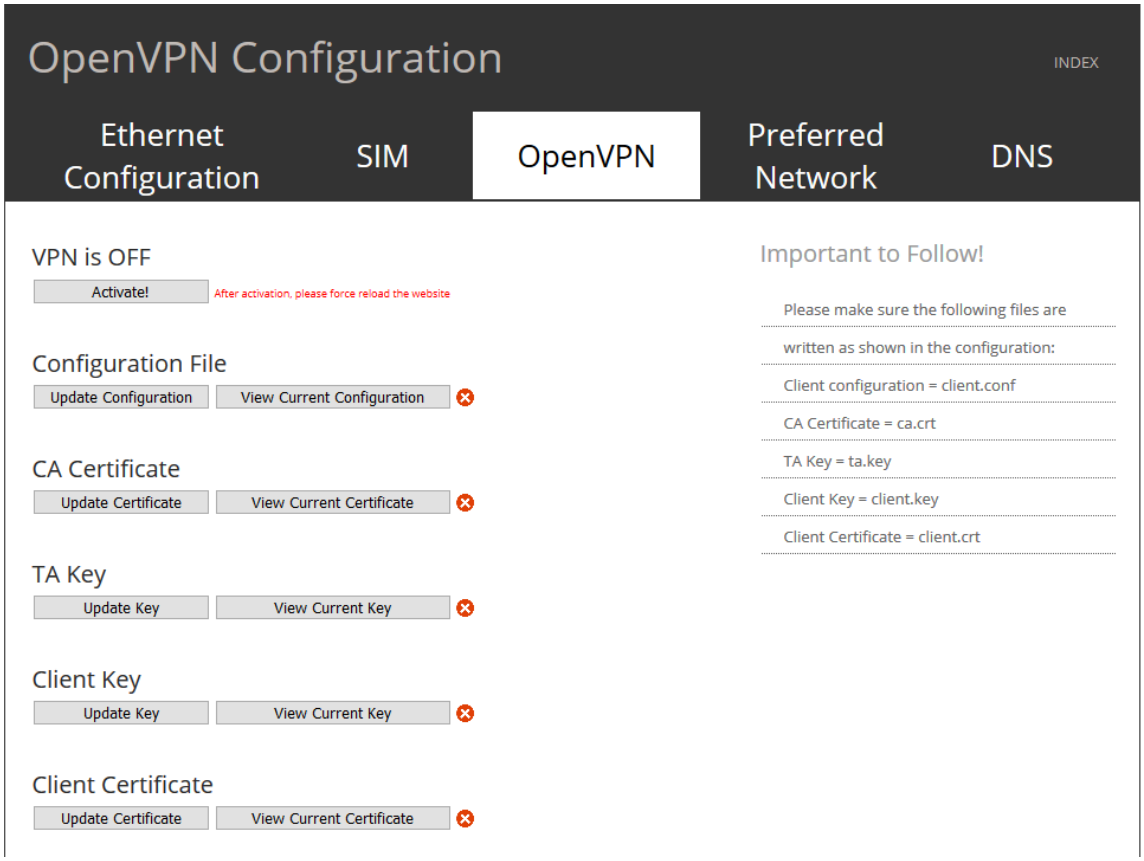
Základní nastavení připojení pomocí VPN vyžaduje pouze vygenerovaný soubor obsahující konfiguraci spojení ze strany klienta směrem k VPN serveru. Konfigurační soubor VPN se do stanice nahraje pomocí integrovaného konfiguračního rozhraní. Úrovně bezpečnosti a požadavků pro navázání VPN tunelu se liší podle konkrétních výrobců dobíjecích stanic a dle podporovaných standardů VPN typů připojení.

Na snímku obrazovky (Obrázek 11) je zachyceno webové konfigurační rozhraní dobíjecí stanice Voltdrive, která podporuje komunikaci s interní sítí pomocí VPN připojení. V tomto případě se jedná konkrétně o podporu OpenVPN.



Obrázek 11— Snímek obrazovky nastavení VPN připojení.Konfigurační rozhraní dobíjecí stanice Voltdrive, zdroj: autor

Nastavení připojení je velice jednoduché a rychlé pouze ve 3 krocích – Povolit službu OpenVPN, nahrát konfigurační soubor a uložit nastavení. Dobíjecí stanice následně sama provede restart síťových zařízení a procesů a následně se připojí k VPN serveru dle nahraného a uloženého konfiguračního souboru.



Obrázek 12— Snímek obrazovky nastavení VPN připojení. Konfigurační rozhraní dobíjecí stanice Alpitronic,zdroj: autor

Snímek obrazovky (Obrázek 12) vyobrazuje sekce nastavení VPN připojení pomocí OpenVPN v dobíjecí stanici Hypercharger od italského výrobce Alpitronic. Ze snímku je patrné, že se jedná o více propracovanou a komplexnější metodu připojení, protože stanice vyžaduje mimo standardního konfiguračního souboru také nahrání klíčů, certifikátů klienta a certifikační autority. Po nahrání všech požadovaných položek a restartu stanice dojde k automatickému restartu jako u stanice Voltdrive a následnému navázání tunelu.

Pokud dobíjecí stanice nepodporuje metodu připojení pomocí VPN spojení, je možné absenci funkce vyřešit instalací externího routeru s modemem a možností VPN připojení. Při testech a v běžném provozu se osvědčil router MikroTik LtAP mini LTE, který disponuje 2G/3G/LTE modemem a je tedy vhodný do všech oblastí pokrytých mobilním signálem.

Mimo připojení pomocí OpenVPN podporuje také VPN typu L2TP/IPSec a IKEv2. Je možné navázat spojení i přímo na Cisco IOS router, takže je velmi vhodný i pro firemní použití. Mezi přednosti routeru patří i možnost vysílání Wi-Fi připojení pro zákazníky čekajících v elektromobilech, nebo pro poskytnutí internetového připojení pro platbu za dobíjení pro neregistrované zákazníky pomocí on-line platby. Router je možné napájet pomocí microUSB nebo napájecím adaptérem v rozmezí 8-30 V, případně pomocí PoE napájení. Router je tak velmi flexibilní pro použití v různých stanicích vybavených odlišnými možnostmi poskytnutí napájení. Velká flexibilita routeru je vyvážena cenou pohybující se okolo 3.000,- Kč[6]. Metoda připojení pomocí přídavného routeru s VPN se tedy vyplatí pouze v situacích, kdy není možné použít řešení konektivity jinými způsoby.

4.2.4 Připojení pomocí SIM s veřejnou IP adresou

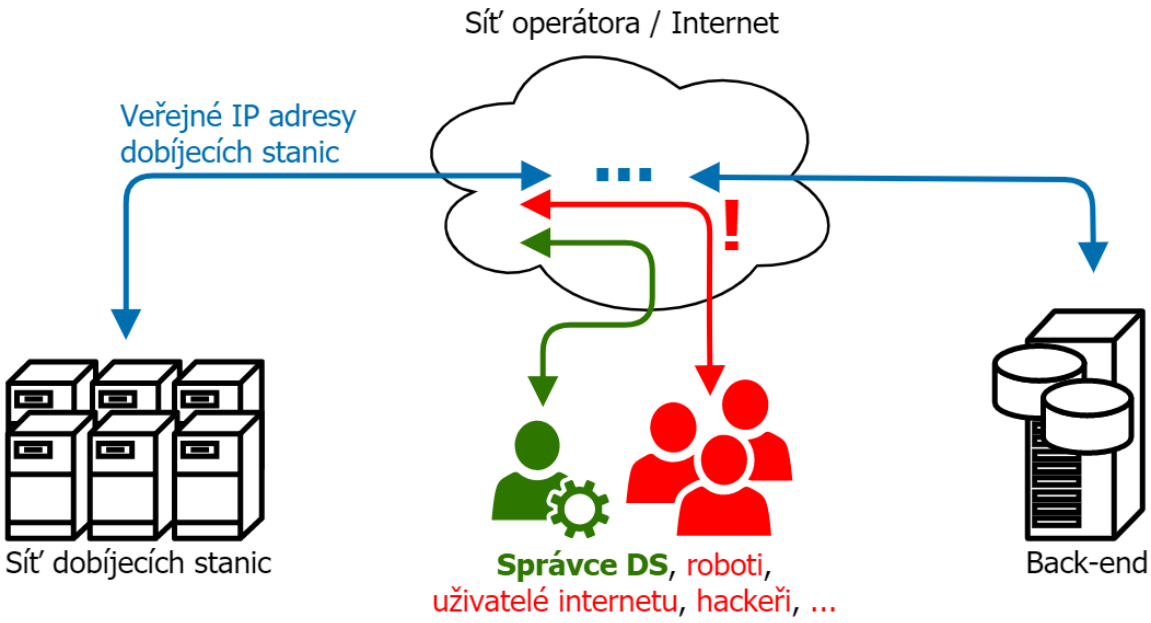
Pro připojení pomocí veřejné IP adresy je nutné vyžádat si u mobilního operátora veřejnou IP adresu, která bude neměnná, tedy statická. Pokud by se jednalo o veřejnou dynamickou IP adresu – adresa není pevně přiřazena a může se po určitém čase změnit –, byla by nutná implementace skriptu, který by pravidelně zjišťoval aktuálně přidělenou adresu a v případě změny by tuto změnu ohlásil správci. Služba zřízení veřejné IP adresy je běžně zpoplatněna měsíčním paušálem, který se odvíjí od zvoleného mobilního operátora nebo poskytovatele služby.

Použití metody s veřejnou IP adresou zajišťuje nejen běžné připojení do internetu, ale zároveň umožňuje i připojení k dobíjecí stanici odkudkoli ze sítě Internet, právě díky veřejné adrese, která není skrytá za překladem síťových adres (zkr. NAT) viz *Obrázek 13*. Tento způsob připojení dovoluje přímou komunikaci mezi dobíjecí stanicí, centrálním systémem
pro správu dobíjecích stanic, a především také se správcem stanic v případě nutnosti komplexnější konfigurace stanice nebo nutnosti diagnostiky. Způsob připojení stanice do sítě je totožný s metodou připojení pomocí SIM karty s veřejným internetem.

[6] Orientační cena routeru zjištěná na e-shopu prodejce i4wifi.cz

Odkrytí IP adresy dobíjecí stanice má své úskalí, protože pokud je možné přistoupit ke stanici odkudkoli z internetu, může tak učinit kdokoli, kdo bude znát její konkrétní internetovou adresu. Dobíjecí stanice se tak může stát potencionálním cílem útoku robotů nebo konkurence. Možností, jak útokům předejít je doplnit do dobíjecí stanice síťové zařízení, které obsahuje firewall a další funkce, které dokáží hrozbu identifikovat a eliminovat (IDS a IPS systémy[7]). Jedná se o přídavné externí zařízení v řádech tisíců korun a při větším počtu dobíjecích stanic se může jednat již o cela nevýhodné řešení z hlediska celkových finančních nákladů.

Potencionální hrozba a vysoké náklady na zabezpečení snadno převažuje výhodu možnosti vzdáleného připojení k dobíjecí stanici nebo vlastní technologickou nenáročnost připojení stanice do sítě. Volba tohoto druhu spojení je převážně vhodná pouze pro testovací účely, pokud je požadavek zajistit možnosti přístupu do rozhraní více zúčastněným stranám nebo se jedná o jedinou možnost, jakým lze připojit stanici do sítě. Připojení pomocí SIM karty s veřejnou IP adresou by mělo být zařazeno tedy pouze jako záložní nebo dočasné řešení komunikace.



Obrázek 13— Zjednodušené schéma připojení pomocí veřejné IP adresy, zdroj: autor

[7] Vysvětlení IDS/IPS systémů Intrusion prevention systém, https://www.systemonline.cz/clanky/intrusion-prevention-system.htm

4.3 Chování dobíjecí stanice při výpadku sítě

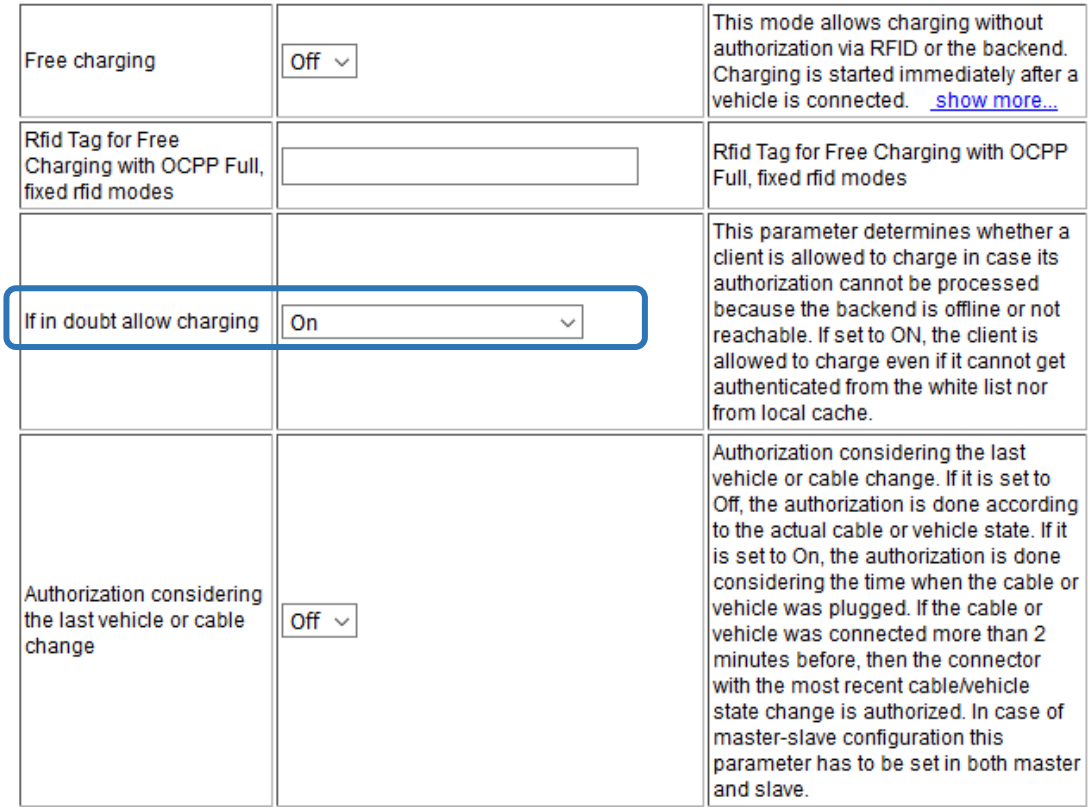
V případě nedostupnosti stabilního síťového připojení nebo jeho výpadku je nutné, aby bylo na dobíjecích stanicích možné zahájit dobíjení elektromobilu. Autorizace uživatele probíhá na straně serveru a je tedy důležité spojení s ním anebo zaručení adekvátního chování při nemožnosti uživatele autorizovat proti back-endu.

Každá dobíjecí stanice má omezené množství možností, které umožňují konfiguraci nastavení, jak se má konkrétní stanice při výpadku konektivity zachovat. Zejména nejpoužívanější jsou metody *lokální cache*, *free charge* a *dobíjení s následnou autorizací* – všechny zmíněné způsoby jsou deklarovány komunikačními protokoly OCPP a detailně popsány v dokumentaci [8][9].

4.3.1 Free charge režim

Nejžádanějším způsobem, jak zajistit možnost dobíjení i při výpadku spojení s back-endem je takzvaný free charge režim (režim volného dobíjení). Nastavením režimu volného dobíjení je umožněno dobíjení elektromobilu i přes nemožnost autorizovat uživatele pomocí zaslání identifikátoru z čipové karty uživatele back-endu. Výhodou je nemožnost rozpoznání uživatelem na první pohled, jestli je stanice off-line nebo online. Nemělo by snadno dojít ke zneužití, kdy uživatel úmyslně přiloží neplatnou kartu, a přesto by mu bylo umožněno zahájení dobíjení.

Modelový příklad je vysvětlen na základní konfiguraci dobíjecí stanice výrobce Ensto. U většiny stanic je konfigurace volného dobíjení otázkou několika málo kliknutí a stejně tomu tak je i v případě tohoto výrobce. Pro aktivaci režimu volného dobíjení v případě nedostupnosti centrálního serveru slouží parametr *If in doubt allow charging* s hodnotou *ON* (Obrázek 10). Nastavením tohoto parametru dojde k zajištění funkčnosti i při výpadku konektivity. Pokud uživatel připojí vozidlo, mávne čipovou kartou před čtečkou a není možné se spojit s back-endem, stanice zahájí dobíjení.



Obrázek 14 — Snímek obrazovky nastavení režimu dobíjení. Konfigurační rozhraní dobíjecí stanice Ensto, zdroj: autor

4.3.2 Dobíjení a následná autorizace

Další možností zajištění provozuschopnosti dobíjecí stanice je povolení dobíjení a následné autorizace při úspěšném navázání spojení s back-endem. V nitru se pod touto funkcí skrývá režim volného dobíjení s nadstavbou dodatečné autorizace uživatele a následného pokračování dobíjení nebo případně zastavení aktuální transakce. Mohou nastat dvě situace. Uživatel připojí vozidlo, mávne čipovou kartou před čtečkou, dobíjecí stanice automaticky zahájí dobíjení. Jakmile se podaří stanici opětovně připojit k centrálnímu systému, autorizuje kartu uživatele – nyní jsou dvě možnosti zachování stanice: při úspěšné či neúspěšné autorizaci pokračuje dobíjecí stanice v dobíjení připojeného vozidla; při zamítnutí karty systémem dojde k přerušení aktuálního dobíjení na daném konektoru.

Modelový příklad si ukážeme na konfiguraci dobíjecí stanice výrobce Alpitronic. Konfiguraci povolení dobíjení a následné autorizace při obnovení spojení nemá každý model stanice dostupný v konfiguračním rozhraní – v některých případech nastavení chybí, protože není výrobcem implementováno, nebo se jedná o výchozí chování stanice a je vloženo přímo (tzv. Hard-coded) do kódu dobíjecí stanice.

Nastavení se provádí pomocí nastavení parametru *AllowOfflineTxForUnknownId* na hodnotu *True* a paramteru *StopTransactionOnInvalidId* na hodnotu *True*, nebo *False* dle požadovaného zachování při neúspěšné autorizaci čipové karty uživatele (Obrázek 15).

V případě parametru *StopTransactionOnInvalidId* se pomocí hodnoty odlišuje pouze způsob ukončení nabíjení, v obou případech ale stanice ukončí aktuální dobíjení vozidla. Pokud je hodnota nastavena na *False*, dojde pouze k odstavení toku elektřiny směrem do vozidla. Při nastavení na *True* dojde k regulérnímu ukončení transakce dobíjení pomocí *StopTransaction*.

AllowOfflineTxUnknownId	true	When set to true, all NFC cards are accepted if the charger is offline. This allows unlimited access to charging capabilities.
AuthorizationCacheEnabled	false	If this key reports a value of true, the Authorization Cache is enabled.
AuthorizeRemoteTxRequests	false	If this key reports a value of true, the Charger will attempt to authorize the NFC Card.
StopTransactionOnEVSideDisconnect	true	When set to true, the Charge Point SHALL administratively stop the transaction when the cable is unplugged from the EV.
StopTransactionOnInvalidId	true	Whether the Charge Point will stop an ongoing transaction when it receives a non- Accepted authorization status in a StartTransaction.conf for this transaction.
StopTxnAlignedData	0	Clock-aligned periodic measurand(s) to be included in the TransactionData element of StopTransaction.req MeterValues.req PDU for every ClockAlignedDataInterval of the Transaction.
StopTxnSampledData	0	Sampled measurands to be included in the TransactionData element of StopTransaction.req PDU, every MeterValueSampleInterval seconds from the start of the charging session.

Obrázek 15— Snímek obrazovky nastavení autorizace dobíjení. Konfigurační rozhraní dobíjecí stanice Alpitronic, zdroj: autor

4.3.3 Lokální cache

Třetí možností je povolení lokální cache neboli paměti pro čipové karty a čipy. Jedná se o seznam, který stanice udržuje v paměti a dle nastavení autorizuje kartu zákazníka oproti tomuto seznamu v případě ztráty komunikace s back-endem, anebo i v online režimu pro rychlejší odbavení zákazníka v případě pomalejšího připojení (způsobeno například slabým signálem nebo absencí LTE pokrytí). Způsob použití lokální cache se lehce liší u každého výrobce dobíjecích stanic. Do některých stanic je nutné tento seznam nahrát a spravovat ručně. Častější možností je automatické stahování seznamu zákaznických identifikátorů z centrálního systému pro správu stanic a správu zákazníků.

Dobíjecí stanice může také fungovat v učícím se režimu a ukládá pouze identifikátory uživatelů, kteří alespoň jednou na konkrétní stanici dobíjeli a došlo k úspěšné autorizaci proti back-endu. Do stanic je možné nahrát nejen seznam povolených identifikátorů, ale i seznam blokovaných. Bohužel v případě použití lokální cache může nastat problém, pokud dojde k naplnění celkového maximálního limitu lokálně uložených karet. Může se tedy stát, že stanice nebude schopná uložit všechny karty a v případě ztráty spojení se serverem by nedošlo k autorizaci uživatele a nebylo mu umožněno dobíjení.

Dle požadavků oddělení eMobility, aby bylo umožněno dobíjení v případě výpadku komunikace, vyplývá, že se jedná o ne úplně vhodný způsob autorizace zákazníka v off-line režimu. Vhodnější je tedy použití předchozích dvou metod.

4.4 Vzdálené ovládání dobíjecí stanice

Vzdálené ovládání stanice je realizováno ze strany systému pro správu dobíjecích stanic. Pro konfiguraci stanic se využívá příkazů *RemoteStartTransaction*, *RemoteStopTransaction*, *UnlockConnector*, *ChangeAvailability* a *Reset* (soft / hard).

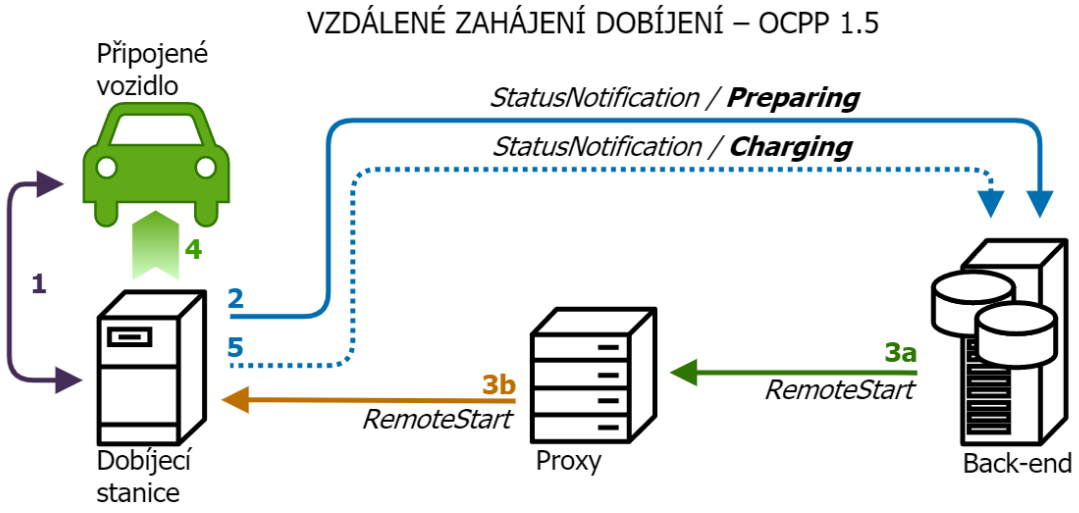
Podmínkou možnosti vzdáleného ovládání stanice je její dostupnost na síti a podpora zasílání příkazů ze strany back-endu. Způsob vzdáleného ovládání se lehce odlišuje dle zvoleného způsobu připojení a použitého protokolu OCPP. V případě použití OCPP 1.5 je vyžadován jako prostředník proxy server (důvod použití proxy serveru v sekci 3.*1.1*

OCPP 1.5), při užívání OCPP 1.6 nutnost prostředníka zaniká a komunikace je uskutečněna díky obousměrnému komunikačnímu tunelu mezi dobíjecí stanicí a back-endem.

Modelový příklad rozebírá způsob ručního vzdáleného zahájení a ukončení dobíjení ze strany operátora obsluhujícího systém pro správu dobíjecích stanic. U dalších příkazů pro ovládání je postup a chování obdobné. Vždy se jedná o sekvenci zpráv, které potvrzují změnu stavů dobíjecí stanice na základě interakce s dobíjecí stanicí ze strany zákazníka a reakcí na povely zaslané operátorem ze strany systému.

4.4.1 S použitím proxy serveru – OCPP 1.5

Po připojení vozidla k dobíjecí stanici, viz *Obrázek 16*, dochází ke komunikaci mezi stanicí a vozidlem (1) a uzamčení dobíjecího konektoru. Následně stanice zašle back-endu zprávu *StatusNotification* (2), která obsahuje detaily o zásuvce dobíjecí stanice a změnu stavu na *Preparing*. Díky informaci o připojení vozidla, nyní může obsluha poslat příkaz na zahájení dobíjení *RemoteStartTransaction*. Back-end odešle zprávu – obsahující informace o zahájení dobíjení, čísla konektoru a identifikaci stanice – proxy serveru (3a), který na základě identifikačního čísla předá zprávu konkrétní dobíjecí stanici (3b). Na základě přijatého povelu zahájí dobíjecí stanice nabíjení vozidla (4) a odešle stavovou zprávu se změnou stavu na *Charging* back-endu (5).

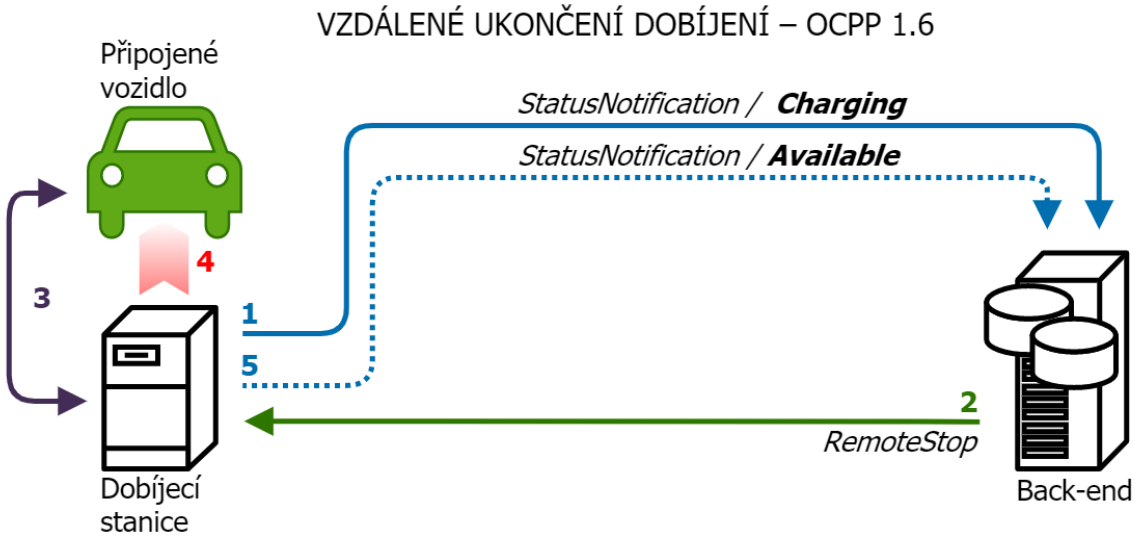


Obrázek 16— Schéma vzdáleného zahájení dobíjení pomocí OCPP 1.5, zdroj: autor

4.4.2 S použitím komunikačního tunelu – OCPP 1.6

V případě obousměrného komunikačního tunelu je zachována stejná funkčnost a možnosti vzdáleného ovládání, ale komunikace je výrazně zjednodušena viz *Obrázek 17*.

Z popisu způsobu vzdáleného zahájení dobíjení je patrné, že po zahájení dobíjení vozidla dojde zaslání stavové zprávy se změnou stavu na *Charging* (1). Pokud operátor potřebuje transakci vzdáleně ukončit, zašle stanici příkaz *RemoteStopTransaction* (2). Stanice na tento příkaz zareaguje a pomocí komunikace s vozidlem (3) ukončí dobíjení a odemkne konektor (4). Následně stanice zasílá back-endu opět stavovou zprávu, nyní ale s informací o změnu stavu na *Available* (5).



Obrázek 17— Schéma vzdáleného ukončení dobíjení pomocí OCPP 1.6, zdroj: autor

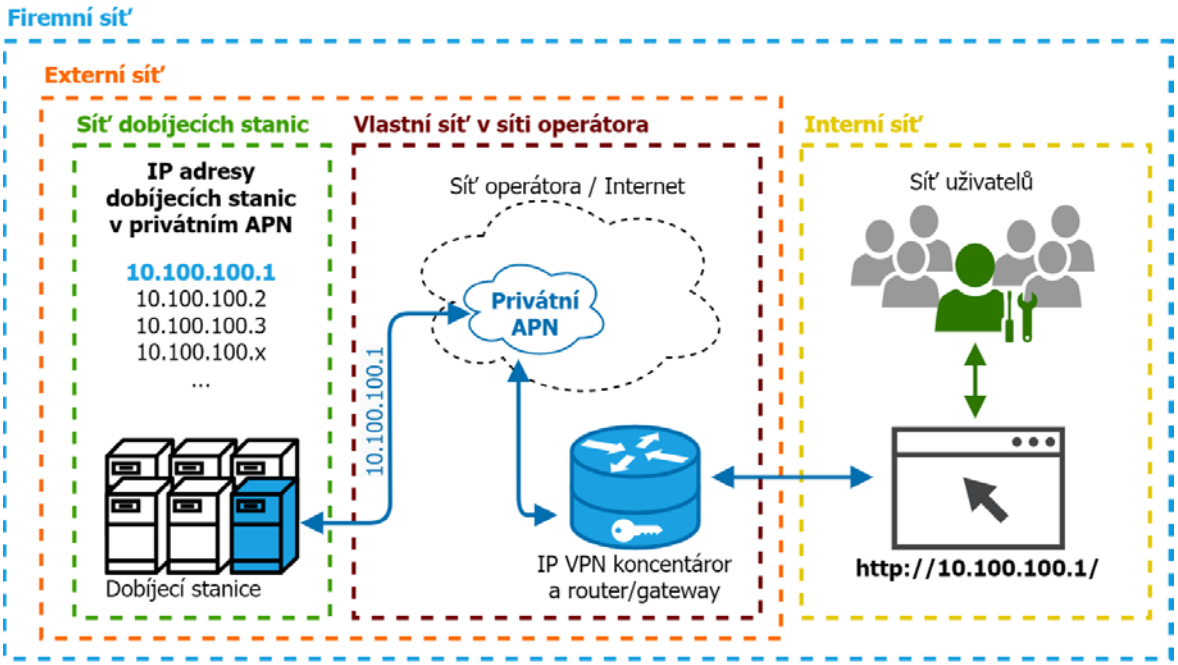
4.5 Vzdálená konfigurace dobíjecí stanice

Pro konfiguraci a úpravu nastavení dobíjecí stanice slouží uživatelské rozhraní, které je dodáváno jako součást systému stanice. V 99 % případů se jedná o grafické webové uživatelské rozhraní, které může být občas doplněno o přístup do textového rozhraní pomocí SSH [12]. Vzdálená konfigurace tak nejčastěji probíhá pomocí použití webového prohlížeče a adresy dobíjecí stanice, anebo pomocí příkazu *GetConfiguration* a *ChangeConfiguration* zaslaného z back-endu.

4.5.1 Konfigurace pomocí rozhraní dobíjecí stanice

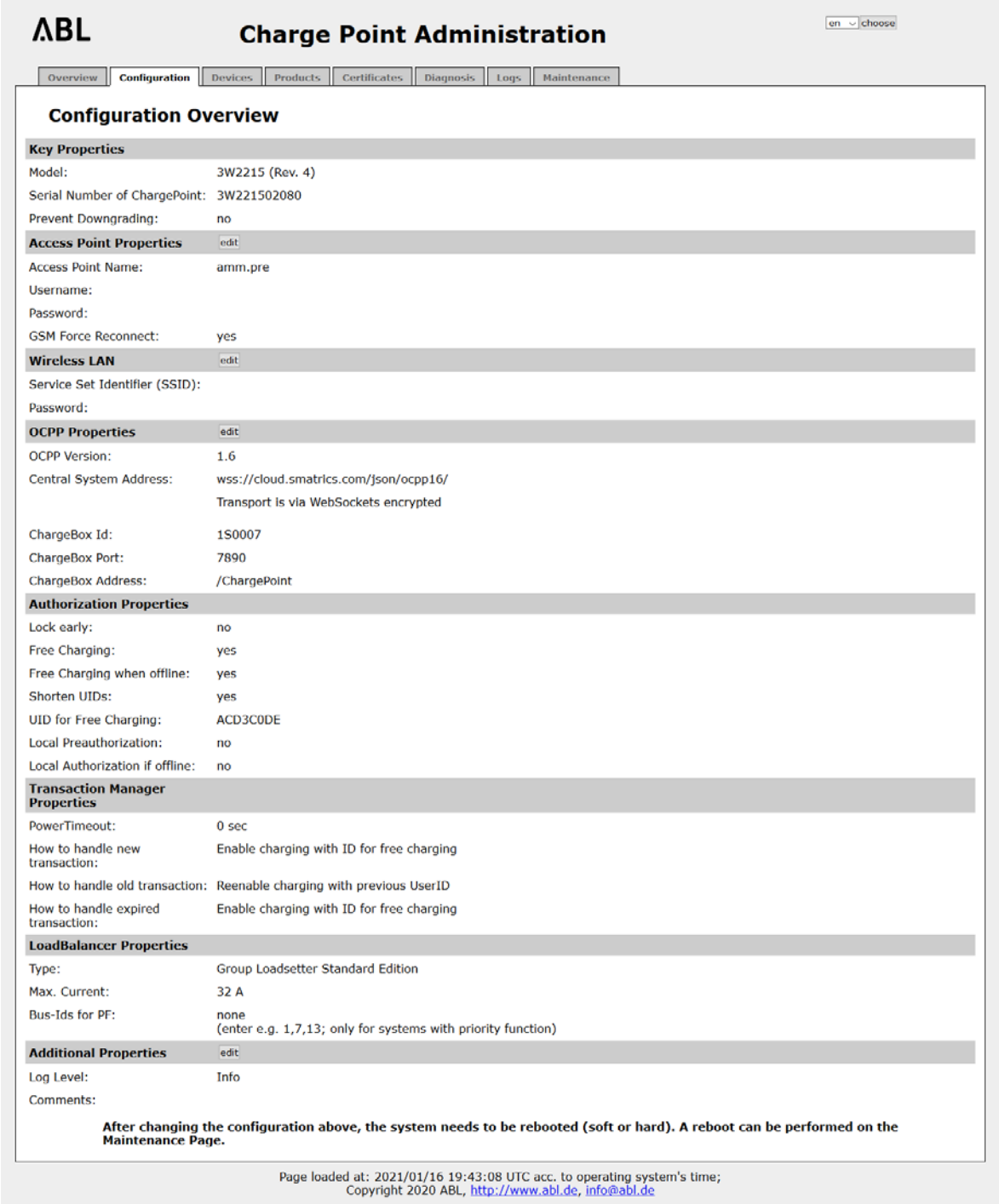
Nejčastěji používaným způsobem konfigurace je systémové rozhraní dobíjecí stanice. Přímé spojení s dobíjecí stanicí lze zajistit při použití doporučených způsobů připojení stanic do síťové infrastruktury (privátní APN, VPN tunel nebo použití veřejné IP adresy). V případě použití jiného typu připojení, například pouze přes síť internet bez veřejné IP adresy nebo bez použití VPN, je nemožné navázat komunikaci pro přímý přístup do konfiguračního rozhraní stanice.

V případě použití doporučených způsobů připojení do sítě, kdy se dobíjecí stanice stávají právě součástí vnitřní infrastruktury, dostačuje, pokud je správce připojen do datové sítě, a má k dispozici běžný webový prohlížeč a zná IP adresu konkrétní dobíjecí stanice (Obrázek 18).



Obrázek 18— Zjednodušené schéma připojení ke konfiguračnímu rozhraní dobíjecí stanice, zdroj: autor

Správce ve webovém prohlížeči do URL adresního řádku zadá IP adresu dobíjecí stanice (např. 10.100.100.1) a potvrdí. Díky propojení sítě dobíjecích stanic do infrastruktury dojde k nasměrování požadavku až k samotné dobíjecí stanici a správci je zobrazeno webové konfigurační rozhraní. Na příkladu je vyobrazeno základní konfigurační rozhraní stanice ABL.

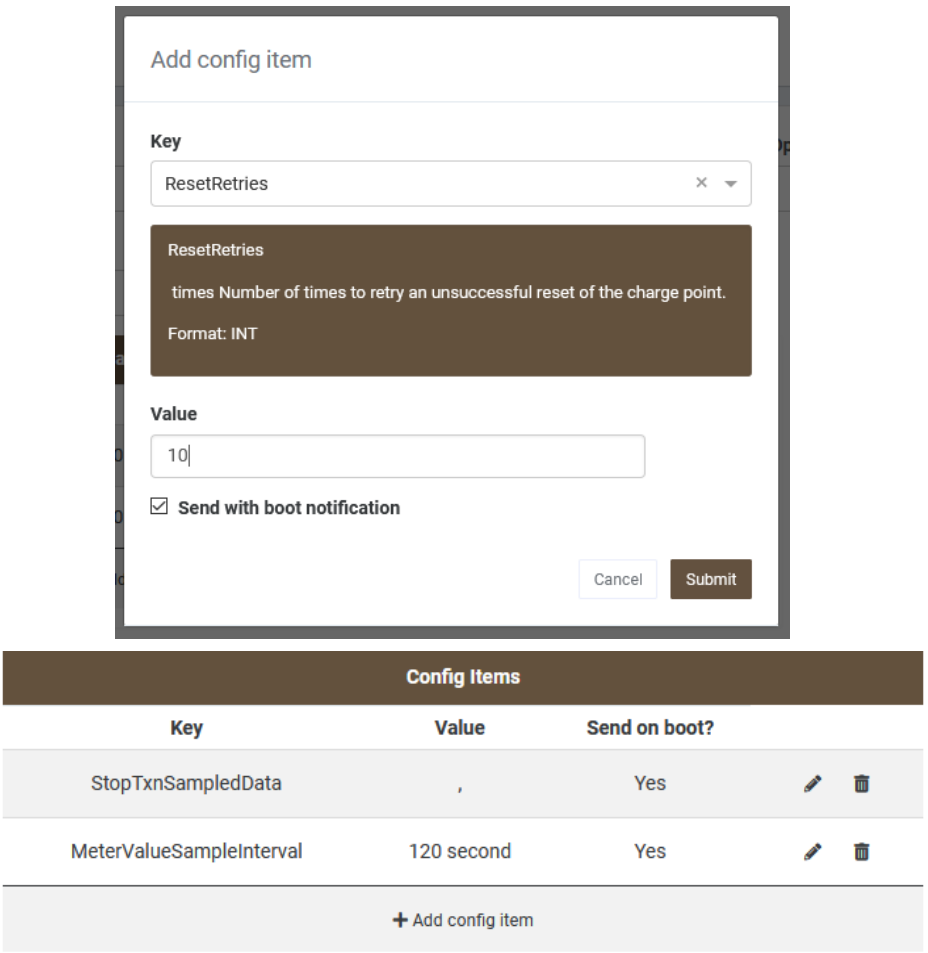


Obrázek 19— Snímek obrazovky konfiguračního rozhraní dobíjecí stanice ABL, zdroj: autor

4.5.2 Konfigurace pomocí back-endu

Konfigurace pomocí back-endu může proběhnout pouze, pokud back-end a dobíjecí stanice umožňují tuto metodu nastavení pomocí protokolu OCPP. Pro vzdálenou konfiguraci se využívají příkazy *GetConfiguration* pro vypsání veškeré konfigurace dobíjecí stanice a *ChangeConfiguration,* který umožňuje upravit hodnotu parametru nastavení. Jedná se o textové zprávy a příkazy, které jsou obdobné, jako příkazy pro vzdálené ovládání.

Pro změnu konfigurace slouží v back-endu pole *Config Items.* Způsob úpravy nastavení je znázorněn na parametru *ResetRetries,* který slouží k opakování neúspěšného resetu nabíjecího bodu. Příkaz pro změnu zasílá back-end ve formátu *ChangeConfiguration(key, value).* Pro nastavení parametru *ResetRetries* dochází k vybrání ze seznamu dostupných parametrů parametr (klíč) ResetRetries a jako hodnotu stačí doplnit počet opakování. V tomto příkladě tedy klíčem bude ResetRetries a hodnota 10 – příkaz zaslaný stanici pak bude vypadat následovně *ChangeConfiguration(ResetRetries, 10).*



Obrázek 20— Snímek obrazovky možnosti konfigurace z back-endu / Smatrics CharVIS, zdroj: autor

Pokud dojde k úspěšnému nastavení, odpoví dobíjecí stanice zprávou *Accepted*, v případě neúspěchu vrátí *Rejected*. Veškeré další parametry – např. *StopTxnSampledData* (zaslání všech naměřených hodnot z ukončené transakce) či *MeterValueSampleInterval* (odesílání aktuálních hodnot z elektroměru) se nastavuje obdobným způsobem, jen za použití jiného parametru a hodnoty.

Možnosti konfigurace jsou limitovány povolenými parametry výrobcem dobíjecí stanice. Možnosti se také odvíjí od možností samotného centrálního systému pro správu stanic – některý systém může podporovat práci se všemi parametry (např. OCC Web od NTT Data) anebo je n s omezeným množstvím předem nastavených parametrů (např. CharVIS od společnosti Smatrics). Většina stanic disponuje možností měnit nastavení URL adresy back-endu a identifikátoru dobíjecí stanice. Dle testování mají nejvíce rozsáhlé možnosti nastavení stanice výrobců Ensto a Alpitronic.

5 Výsledky a diskuse

5.1 Požadavky IT a správy eMobility

Mezi základní a zároveň nejdůležitější požadavky oddělení správy IT a oddělení eMobility patří možnost vzdáleného připojení do dobíjecí stanice a možnost konfigurace pomocí webového rozhraní. Správci eMobility zároveň požadují zajištění možnosti dobíjení elektromobilu i v případě výpadku konektivity s dobíjecí stanicí, kdy není možné autorizovat zákazníka proti centrální databázi čipových karet zákazníků.

Ze strany IT oddělení jsou požadavky na zajištění základní bezpečnosti připojení. Zejména, aby byla dobíjecí stanice chráněna před hrozbami v síti internet a nebyla umožněna správa neoprávněné osobě – například ochrana webového konfiguračního rozhraní pomocí jména a hesla. Dalším požadavkem ze strany správy IT, jakožto techniků starajících se o bezproblémovou komunikaci a oživování nových dobíjecích stanic je flexibilita připojení pro snadnou implementaci dobíjecích stanic různých výrobců do síťové infrastruktury.

Posledním požadavkem je možnost monitoringu výpadků konektivity dobíjecích stanic, realizovanou například dohledovým systémem Zabbix nebo NNMi.

5.2 Doporučený způsob připojení do sítě

Doporučený způsob připojení stanic do síťové infrastruktury se liší podle počtu spravovaných dobíjecích stanic, počtu používaných výrobců stanic, geografickou rozlohou stanic a náklady spojenými s provozem (Tabulka 1, strana 52).

Pro velký počet (50 a více) dobíjecích stanic je vhodné použití připojení pomocí privátního APN u operátora. Jedná se o nejnákladnější způsob připojení, který je ale nejsnadnější udržovat. Zároveň se jedná o nejflexibilnější způsob připojení do sítě, protože je realizován pouze pomocí datové SIM karty a nevyžaduje další funkce jako VPN. Lze jej hodnotit i jako ideální nástroj na sjednocení způsobu připojení při rozmanitém výběru stanic mnoha výrobců. Použití vlastního APN také poskytuje dobrou úroveň bezpečnosti,

protože stanice nemají možnost připojit se do internetu a jsou tedy chráněny i před bezpečnostními riziky. Zároveň v případě částečného výpadku stanice pouze od centrálního systému, ale při zachování konektivity do sítě, je možné se k stanici vzdáleně přihlásit a provést manuálně restart.

Pro menší počet spravovaných stanic je vhodné zvolit způsob připojení pomocí VPN tunelu, který nabízí některé benefity jako privátní APN, ale při menších provozních nákladech (Tabulka 1, strana 52). Díky spojení tunelem umožňuje správu stanic pomocí integrovaného webového rozhraní, poskytuje relativně dobrou úroveň bezpečnosti dle použitého protokolu (PPTP vs. IPSec vs. IKEv2). Přes nižší náklady je také zapotřebí počítat s úskalím VPN tunelování. Ne všechny stanice jsou kompatibilní s tímto typem připojení a případnou nekompatibilitu je nutné řešit pomocí doplnění externího zařízení, které podporuje VPN připojení. Jedná se také o připojení, žádající si pravidelnou údržbu jako je aktualizace certifikátů nebo řešení problémů, kdy dojde k rozpadu tunelu a nový tunel není navázán – dobíjecí stanici se rozpadne konektivita s back-endem a není možný ani vzdálený zásah ze strany správce.

Použití připojení pomocí VPN má i své uplatnění v případě, že se stanice nachází například v podzemních garážích, kde mohou vznikat problémy s příjmem mobilního signálu. V tomto případě je vhodné doplnit dobíjecí stanici o router podporující VPN spojení (například routery Mikrotik) společně s připojením k internetu od lokálních poskytovatelů pomocí kabelových technologií anebo bezdrátové technologie Wi-Fi.

Posledním akceptovatelným a možným způsobem připojení je využití SIM karty s veřejnou statickou IP adresou. Tento typ připojení lze doporučit pouze pro speciální případy, kdy není možné použít připojení pomocí privátního APN nebo VPN. Jedná se o nejméně bezpečný způsob, protože stanice je vystavena hrozbám z internetu a nemusí disponovat dostatečnou mírou zabezpečení, aby případným hrozbám byla stanice schopna odolávat. Technicky se jedná o nenáročné řešení, a je možné jej využívat mimo řešení konektivity problémových stanic například na testování, protože díky veřejné IP adrese je konfigurační rozhraní dobíjecí stanice dostupné odkudkoli z internetu a zároveň se nachází síť mimo firemní síťovou infrastrukturu a jsou vytvořeny možnosti otevřeného testování.

5.3 Doporučení konfigurace funkčnosti při výpadku konektivity

Preferovaný způsob zajištění možnosti dobíjení i při ztrátě konektivity s dobíjecí stanicí je využití free-charge režimu v kombinaci režimu dodatečného autorizování dle možností jednotlivých technologií výrobců dobíjecích stanic.

U klasických (AC) dobíjecích stanic [7] je očekáváno použití free-charge režimu bez dodatečné autorizace. V případě výpadku konektivity je tak umožněno dobíjení všem zákazníkům bez rozdílu. Pokud není uživatel dobíjející elektromobil firemním zákazníkem nebo nemá platnou čipovou kartu, je přesto umožněno pokračování v nabíjení i po obnovení konektivity stanice s centrálním systémem.

V případě rychlých (DC) dobíjecích stanic [7] je, pokud to stanice umožňuje, využíváno funkce povolení dobíjení s dodatečnou autorizací po obnovení připojení k systému. Každé připojené vozidlo může během výpadku dobíjet. Pokud dojde k obnovení spojení s centrálním systémem a uživatel je následně úspěšně autorizován, nabíjení pokračuje, pokud dojde k zamítnutí uživatele, je nabíjení ukončeno.

Tabulka 1 – Porovnání jednotlivých způsobů připojení, zdroj: autor. Legenda: výborně ✓, s výhradou !, špatně ✗

Typ připojení / Funkce	SIM / veřejný internet	SIM / privátní APN	SIM / VPN tunel	SIM / veřejná IP adresa
Technologická náročnost	✓	!	!	✓
Finanční náročnost	✓	✗	!	✓
Vzdálená správa	✗	✓	!	✓
Bezpečnost sítě	!	✓	✓	✗
Náročnost integrace				
ABL	✓	✓	!	✓
Alpitronic	✓	✓	✓	✓
Ensto	✓	✓	!	✓
Kostad/Siemens	✗	✗	✗	✓
Voltdrive	✓	✓	✓	✓
Zabezpečení rozhraní				
ABL	✗	!	!	✗
Alpitronic	✓	✓	✓	✓
Ensto	!	✓	✓	!
Kostad/Siemens	✓	✓	✓	✓
Voltdrive	✓	✓	✓	✓
Vhodné pro < 50 stanic	!	!	✓	!
Vhodné pro 50+ stanic	✗	✓	!	✗
Vhodné pro rozhlelou síť	✗	✓	✓	✗
Vhodné pro "lokální" síť	✓	✓	✓	!
Režim volného dobíjení				
ABL	✓			
Alpitronic	✓			
Ensto	✓			
Kostad/Siemens	✓			
Voltdrive	✓			
Režim nabíjení a následné autorizace				
ABL	✓			
Alpitronic	✓			
Ensto	✓			
Kostad/Siemens	!			
Voltdrive	✓			
Podpora OCPP 1.6				
ABL	✓			
Alpitronic	✓			
Ensto	✓			
Kostad/Siemens	!			
Voltdrive	✓			
DOPORUČENÍ	✗	✓	!	!

6 Závěr

V první části bakalářské práce byly zanalyzovány typy a možnosti připojení dobíjecích stanic pomocí SIM karty s veřejným internetem, SIM karty s privátním APN, SIM karty s veřejnou IP adresou, připojením k internetu a použití VPN spojení.

Na základě rozdílů mezi komunikačními protokoly zkoumané v teoretické části práce byla charakterizována problematika odlišných možností připojení stanic různých výrobců a možností dle využitých protokolů OCPP. Ne každý výrobce podporuje totožné možnosti připojení jako ostatní výrobci dobíjecích stanic. U některých výrobců například absence možnosti VPN spojení nebo chybějící možnost zabezpečení konfiguračního rozhraní.

Dle požadavků ze strany poskytovatele služeb dobíjecích míst byly definovány preference oddělení informačních technologií a požadavky oddělení správy eMobility viz kapitola *5.1 Požadavky IT a správy eMobility*.

Na základě provedení testů na dobíjecích stanicích různých výrobců byl navrhnut postup implementace dobíjecích stanic pomocí připojení do sítě využívající konektivitu SIM karty od operátora. Dle výsledků testů byly doporučeny 3 možnosti připojení – preferovaný typ připojení pomocí SIM s privátním APN, využití spojení pomocí VPN tunelu a pro speciální a testovací účely možnost využití SIM karty s veřejnou IP adresou.

S přihlédnutím ke všem technickým požadavkům oddělení informačních technologií a správců eMobility ohledně integrace dobíjecích stanic do síťové infrastruktury a zajištění funkčnosti i přes výpadek konektivity, je nutné přihlédnout i k samotným možnostem dobíjecích stanic. Nejdůležitějším krokem při rozhodování a volbě možností integrace se síťovou infrastrukturou je struktura dobíjecích stanic (Tabulka 1, strana 52).

Pokud se jednoznačné jedná o homogenní strukturu, která bude ve stejné formě udržována do budoucna, je vhodné rozhodnout se na základě použitých technologií a cenové náročnosti. V případě, že by se jednalo o sít heterogenní s velkým počtem odlišných modelů, je vhodné nejprve analyzovat všechny možnosti jednotlivých stanic a následně se rozhodnout, jakým způsobem stanice do sítě implementovat. Důležitou roli hraje

především jednotnost integrace, aby se předešlo použití několika podobných technologií v souběhu.

Vzhledem k rozšiřující se základně uživatelů elektromobilů by nebylo chybou ani pro začínající projekty zainvestovat více do nákladnějšího způsobů připojení pomocí vlastního APN u operátora, protože v budoucnu se tak bude možné vyhnout případným potížím s kompatibilitou či obtížným servisem, vyžadujícím výjezd technika ke každé z dobíjecích stanic.

7 Seznam použité literatury

1. Corzato, G. & Secco, Luca & Rasheed, Arslan & Nagar, Atulya & Secco, Emanuele. *E-Mobility: smart grid and charging session of electric vehicles* [online]. [cit. 2020-06-10]. Dostupné z: https://www.researchgate.net/publication/323967720_E-Mobility_smart_grid_and_charging_session_of_electric_vehicles

2. WIRGES, Johannes. *Planning the Charging Infrastructure for Electric Vehicles in Cities and Regions* [online]. ISBN 978-3-7315-0501-3. [cit. 2020-06-10]. Dostupné z: https://publikationen.bibliothek.kit.edu/1000053253/3877194

3. Orcioni, S.; Conti, M. *EV Smart Charging with Advance Reservation Extension to the OCPP Standard*. Energies 2020 [online]. [cit. 2020-12-28]. Dostupné z: https://www.mdpi.com/1996-1073/13/12/3263/pdf

4. Schmutzler, J.; Andersen, C.A.; Wietfeld, C. *Evaluation of OCPP and IEC 61850 for smart charging electricvehicles.* [online]. [cit. 2020-06-10]. Dostupné z: https://www.mdpi.com/2032-6653/6/4/863/pdf

5. Gaute Ness. *Smart Electric Vehicle Charging System*. [online]. [cit. 2021-01-20]. Dostupné z: https://core.ac.uk/download/pdf/225893174.pdf

6. Venkata Pruthvi, Thota & Dutta, Niladri & Bobba, Phaneendra & Vasudeva, B. *Implementation of OCPP Protocol for Electric Vehicle Applications*. [online]. [cit. 2020-08-15]. Dostupné z: https://www.researchgate.net/publication/331281703_Implementation_of_OCPP_Protocol_for_Electric_Vehicle_Applications/fulltext/5c7005c992851c695038fa17/Implementation-of-OCPP-Protocol-for-Electric-Vehicle-Applications.pdf

7. Robert van den Hoed, Robert & Maase, Simone & Helmus, Jurjen & Wolbertus, Rick & Bouhassani, Youssef & Dam, Jan & Tamis, Milan & Jablonska, Bronia. *E-mobility: getting smart with data* [online]. [cit. 2020-06-10]. Dostupné z: https://www.researchgate.net/publication/334625203_E-mobility_getting_smart_with_data

8. *Home - Open Charge Alliance* [online]. [cit. 2020-05-04]. Dostupné z: https://www.openchargealliance.org/

9. Open Charge Alliance. *Open Charge Point Protocol: 1.5 FINAL* [online]. [cit. 2020-06-10]. Dostupné z: https://www.openchargealliance.org/downloads/

10. Open Charge Alliance. *Open Charge Point Protocol 1.6: 1.6 edition 2 FINAL* [online]. [cit. 2020-06-10]. Dostupné z: https://www.openchargealliance.org/downloads/

11. *Ready for tomorrow's technology | Automation | Siemens Global* [online]. [cit. 2021-01-21]. Dostupné z: https://new.siemens.com/global/en/company/stories/industry/factory-automation/kostad-emobility-charger.html

12. *SOAP Web Services Tutorial: What is SOAP Protocol? EXAMPLE* [online]. [cit. 2021-02-28]. Dostupné z: https://www.guru99.com/soap-simple-object-access-protocol.html

13. *JSON* [online]. [cit. 2021-02-28]. Dostupné z: https://www.json.org/json-en.html

14. *What are WebSockets? | Web Security Academy* [online]. [cit. 2021-02-28]. Dostupné z: https://portswigger.net/web-security/websockets/what-are-websockets

15. *Charge Point Management | SMATRICS* [online]. [cit. 2021-02-28]. Dostupné z: https://smatrics.com/en/node/4631

16. *IoT Hacking Series #11: How do VPN, APN and Fixed IP SIM work? — 1oT - Global Cellular Connectivity for IoT* [online]. [cit. 2021-02-28]. Dostupné z: https://1ot.mobi/resources/blog/vpn-apn-fixed-ip

17. *Připojení M2M a IoT | Top Connect* [online]. [cit. 2021-02-28]. Dostupné z: https://topconnect.com/cs/pripojeni-m2m-a-iot/

18. *Homepage - LoRa Alliance®* [online]. [cit. 2021-02-28]. Dostupné z: https://lora-alliance.org/

19. *Sigfox - The Global Communications Service Provider for the Internet of Things (IoT)* [online]. [cit. 2021-02-28]. Dostupné z: https://www.sigfox.com/en/

8 Seznam obrázků

9 Seznam tabulek

10 Seznam použitých zkratek

APN	*Access Point Name – přístupový bod pro připojení k bráně v síti operátora*
Back-end	*Systém pro správu a monitoring dobíjecích stanic*
DS	*Zkratka pro dobíjecí stanici*
EV	*Zkratka pro vozidlo s pohonem na elektřinu*
GUI, WebUI	*Zkratka pro grafické rozhraní pro konfiguraci dobíjecí stanice*
HTTP, HTTPS	*Hypertext Transfer Protocol pro komunikaci s webovými servery*
IoT	*Zkratka pro Internet of Things (česky Internet věcí)*
IP	*IP adresa (Internet Protocol address) – slouží pro identifikaci každého zařízení v síti*
JSON	*JavaScript Object Notation – standardizovaný formát pro výměnu dat*
OCA	*Open Charge Alliance – správce OCPP protokolů*
OCPP	*Open Charge Point Protocol – protokol pro komunikaci dobíjecích stanic*
SIM	*Subscriber Identity Module – Jedná se o kartu sloužící k identifikaci účastníka v mobilní síti operátora*
SOAP	*Simple Object Access Protocol sloužící pro komunikaci XML zprávami přes http nebo https*
URL	*Uniform Resource Locator – popis umístění webové stránky nebo souboru na internetu*
VPN	*Zkratka pro virtuální privátní síť*
WS, WSS	*WebSocket komunikační protokol pro obousměrnou komunikaci*