NEW WHITE PAPER

Unleash the magic of zero-touch charging: Plug & Charge

Author: Dr. Marc Mültin, CEO & Founder
Published: 8 June 2023

Switch

Table of contents

Introduction

"Any sufficiently advanced technology is indistinguishable from magic,"

declared Arthur C. Clarke, the renowned co-author of “2001: A Space Odyssey.”

While this sentiment holds true for many areas of our lives, it hasn't quite extended to the realm of Electric Vehicle (EV) charging – at least not for all. However, there is a select group of drivers who are already experiencing the enchantment: Tesla drivers. Tesla operates a closed ecosystem with complete control over the hardware and software of their EVs and chargers, delivering a seamless and convenient charging experience to their users.

What if there was a way to expand this seamless experience to all EV manufacturers and charger manufacturers, regardless of brand or geographic location? This is where Plug & Charge, or PnC, enters the stage, an innovative and advanced technology that wholeheartedly embraces the notion of "magic." By seamlessly integrating multiple market roles and orchestrating a flawlessly functioning ecosystem, Plug & Charge sets out to revolutionise the identification and charging process at any charging station, anywhere. The result is improved customer retention and a better business case for businesses embracing this technology.

Plug & Charge is not just another technology; it is an advanced system that transcends the ordinary (or at least not noteworthy). It involves a multitude of market roles and a meticulously crafted ecosystem, all working together to make charging and payment at a charging station truly seamless, just like magic. This user-convenient mechanism is based on the EV-to-charger communication standard ISO 15118. It is achieved by placing a digital certificate inside the EV, eliminating the need for RFID cards, smartphone apps, or credit cards to authorise charging and billing. While ISO 15118 still supports these so-called "External Identification Means" or EIM, Plug & Charge takes us beyond them, into a realm where enchantment rules.

To understand the concept of Plug & Charge, consider Apple Pay, which simplifies payment by enabling contactless transactions through Apple devices. In a similar vein, Plug & Charge eliminates the need for additional steps or authentication procedures in the EV charging process. Just as Apple Pay liberates users from carrying physical cards and streamlines the authentication process, Plug & Charge transforms the EV charging experience into a seamless and effortless endeavour. Further, it brings the automated ease of machine-to-machine communication that is *not* just convenient, but also outstandingly secure. Most importantly, it works with zero driver involvement as payment and billing is authenticated and automated.

The purpose of this white paper is to guide you through the world of Plug & Charge, providing non-experts with the knowledge they need to make informed decisions when embracing this transformative technology into their product and service offerings. We will delve into the inner-workings of Plug & Charge (which is based on the ISO 15118 protocol), explore the creation of a cohesive ecosystem with its various roles, discuss methods of achieving interoperability among different providers, and address common misconceptions surrounding Autocharge.

Furthermore, I am excited to introduce you to a Plug & Charge solution that is ready to propel both charger manufacturers and operators of charging station networks into the future. At Switch, we have intentionally chosen to lead the way, pushing the boundaries of technological development to create the most powerful and seamless solution yet. Our aim is to help you build superior EV charging networks, ones that carry real market value for your business and benefit your customers. With Plug & Charge, you gain a competitive advantage that pushes your business to the next level.

I invite you to explore the possibilities this advanced system offers for your charging station networks. Reach out to me at marc@switch-ev.com, and let me show you how our Plug & Charge solution can transform your business. My team of experts is eager to discuss your unique requirements and showcase the capabilities of our Plug & Charge solution.

I'm looking forward to guiding you through the possibilities of zero-touch charging!

Warm regards,
Marc

Acknowledgements

What set out to be a succinct white paper of maybe 20 to 30 pages to provide a brief overview of the Plug & Charge ecosystem has now turned into a quite comprehensive technology report. This has become a carefully crafted brain dump of pretty much all my knowledge on Plug & Charge. But I couldn't have it done without the support and input of some of my industry peers and my valued Switch team members. I'd like to extend my deepest gratitude to everyone who contributed content or insider knowledge.

Let me specifically call out Steffen Rhinow (Director Plug & Charge at Hubject), Glenn Cezanne (Head of Public Affairs, EU at CharIN), Ben Kegler (Marketing & Communications Director at Switch), Eve Marie-Röseler (Head of Content at Switch), Adam Chilab (CPO at Switch) and André Duarte (CTO at Switch).

The cover image of this white paper has been designed by our talented Sou Yee Chung, Head of Brand at Switch.

Last but not least, I'd like to thank everyone who asked questions and provided comments when I prompted my followers on Linkedin, which Plug & Charge topics are most relevant to them. This heavily influenced the direction of this white paper.

The current EV charging experience is messy

The current EV charging ecosystem is heavily fragmented and, as a result, the charging experience for the EV driver is often reported as being a frustrating disappointment.

The University of California, Berkeley conducted a study in April 2022 that finds more than a quarter of 657 public DC fast chargers non-functional. The main failures are unresponsive screens, broken connectors, payment system issues, failed charging initialisations and unreliable communications between chargers and their backend systems.

Imagine the outcry if every one out of four times you try to fuel up your petrol car you're stuck with some issues at the gas station. Why should that be acceptable for the EV charging industry? Clearly we need to do better.

Regarding payment, third-party authentication methods such as membership RFIDs, credit cards or mobile apps are not just a security risk but also tend to have issues such as being out of service as they are not built to a reliable standard. Also, mostly low quality NFC chips with poor transactional security are used. In February 2022, a study published by iNews, who monitored comments on Zap-Map's Zap-Chat over a two-week period in December 2021, revealed a staggering 30% of charging events had failed – leaving EV drivers frustrated and without battery power.

In many ways, the EV charging industry resembles the telecommunications industry. Take 'roaming', for example. Roaming facilitates the communication between those operating and maintaining the (charging) network and those holding the contractual relationship with the end user to provide access to this network. Currently, access to charging stations is provided using either RFID cards/fobs or apps that need to be first downloaded and installed on your smartphone. The more service providers that only cover part of the network, the more RFID cards you need to carry in your wallet or apps you need to install. Clearly, this approach doesn't scale, it's quite frankly the opposite of a user-friendly system design.

The only action an EV driver should be supposed to take is to plug in the cable – or when we talk about wireless charging, park above a wireless charging pad. That should be it. The EV should identify and authorise itself to the charger on behalf of the EV driver – in a secure way, no further interaction required.

But how do we achieve this?

Introducing Plug & Charge – The foundation for a seamless charging experience

Whenever machines are supposed to 'talk' to each other in a secure way, we need to think about confidentiality, data integrity and authenticity. They are the three pillars of secure digital communication:

1. **Confidentiality**: Your EV needs to talk to the charging station (or wall box) and make sure that no unauthorised third party can listen in on the conversation

2. **Data Integrity**: The data that the EV and charging station exchange must be secure, and any malicious third-party attempts to manipulate the conversation must be detected on both sides

3. **Authenticity**: The EV must identify and be able to verify the charger to which it is physically connected as a trustworthy charger, and vice versa

The big value of Plug & Charge lies in the fact that businesses can offer their customers a secure and seamless charging experience without compromising on data security (as opposed to Autocharge).

So far, so good. But the question still remains: How do we facilitate this?

That's where we enter the realm of data encryption, digital signatures and digital certificates. And with it comes a whole ecosystem comprising a set of roles, policies and procedures. They are needed to create, manage, distribute, use, store and revoke digital certificates. We call this a Public Key Infrastructure, or PKI for short.

This is the type of content I usually teach in the *Advanced Training* sessions part of the "Charging Communications with ISO 15118" organised by CharIN Academy. For the purpose of this white paper, I aim to provide a succinct overview of the complete Plug & Charge ecosystem and the underlying process behind a Plug & Charge session.

While the structure of the Plug & Charge specific PKI with all its certificates is defined in ISO 15118, its governing rules are set in the application rule VDE-AR-E 2801-100-1, titled "Handling of certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO 15118."

As the title suggests, it's not just the EV and the charging infrastructure but also a series of players and procedures in the background that need to be carefully orchestrated to make the "Plug & Charge-magic" happen.

Here's an overview of all the involved market roles:

- The electric vehicle (EV)
- The EV manufacturer (here: OEM)
- The charging station
- The Charge Point Operator (CPO)
- The Mobility Service Provider (MSP, also known as Mobility Operator, or MO)
- The operator of the V2G Root CA (CA = Certificate Authority)
- The operator(s) of the necessary data pools and cloud-based services that need to be in place to facilitate the provisioning of certificates to enable Plug & Charge

Each and every market role within this ecosystem must be assigned a unique certificate that identifies them as an authentic and trustworthy party in an ecosystem that needs to operate like clockwork – irrespective of the EV or charger brand and location.

Before we take a closer look at how the Plug & Charge process works in detail, I'll first explain a few cryptography basics first.

Plug & Charge requires a Transport Layer Security (TLS)-encrypted communication between EV and charging station. It's important to properly understand this most complex part of ISO 15118, especially when you're tasked with its implementation or interoperability and conformance testing.

You'll read a lot about digital certificates, digital signatures and PKIs in this white paper. If this is all new to you, I strongly suggest you take the time to dive into the following section. If you're already familiar with these concepts, then feel free to skip the following chapter.

Cryptography basics of Plug & Charge

In this chapter, you'll get the abbreviated version of what I usually teach in the Advanced Training sessions on ISO 15118 communication. If you'd like to dig deeper, you might want to check out the Academy website for the next CharIN Academy training and registration details.

Encrypting the communication with TLS

To establish confidentiality between the EV and the charging station, we need to encrypt the data they exchange during a charging session. And that's where TLS, or Transport Layer Security, comes into play.

TLS is a protocol that provides secure communication over TCP[1]-based communication channels like the internet. It is used to encrypt data that is being transmitted between a client (such as a web browser) and a server (such as a website). In our EV charging scenario, the client is the EV, the server is the charging station, and the TCP-based communication channel is either a Wi-Fi channel for e.g. wireless charging or the charging cable that transmits data via power line communication (PLC).

When a client (EV) connects to a server (charger) using TLS, they establish a secure connection by performing a 'handshake' process. During the handshake, the EV and the charger exchange information and agree on a shared encryption key that will be used to encrypt and decrypt data during the charging session.

Once the secure connection is established, any data transmitted between the EV and charger is encrypted and cannot be read by anyone who may be monitoring the communication. This makes TLS an important tool for protecting sensitive information, such as authentication data or charging schedules.

The shared encryption key is also known as the TLS session key, or a symmetric session key. It's called a 'symmetric key' because the same key is used to both encrypt and decrypt the data on both sides. The algorithm used to encrypt and decrypt data in ISO 15118 is known as Advanced Encryption Standard, or AES. It has been widely used for many decades across various applications. ISO 15118-2 uses 128 bit symmetric keys, which is why the symmetric cipher is called AES-128-CBC. The trailing 'CBC' stands for Cipher Block Chaining mode, which is one of several modes of operation with the symmetric cipher AES.

[1] TCP stands for Transmission Control Protocol and is a fundamental protocol for reliable data transfer, ensuring that all data is delivered to the receiver without errors or loss. It is used by many applications, including web browsing, email, file transfers, and streaming media.

The case for Public Key Cryptography

Symmetric keys and ciphers enable us to encrypt and decrypt the communication. But what if someone was tapping the communication channel (like the charging cable between the EV and charger) during the TLS handshake? Wouldn't that person then be able to intercept the symmetric TLS session key that the EV and the charger are exchanging? If that's the case, then the eavesdropper would be able to listen in on the communication, and the whole purpose of TLS would be rendered useless.

The eavesdropper could even go one step further and try to manipulate the communication by intercepting data, modifying it, and injecting the modified data for some malicious purpose like manipulating charging schedules (e.g. to induce a blackout) or authentication data (e.g. to charge on behalf of someone else's account). How would the EV or charger know if they're actually talking to a trustworthy party and not falling prey to this kind of man-in-the-middle attack?

That's where public key cryptography comes to the rescue.

Public key cryptography is based on the principle of a mathematically related key pair, of which one is called the private key and the other is called the public key. The private key must be kept secret at all times, otherwise the key pair is considered to be compromised. The public key is made available to other communication partners. It's a versatile tool that can be used for various cryptographic applications, including encryption/decryption, key agreement, and digital signatures. In the realm of EV charging, we use this tool only for agreeing on a TLS session key and for digital signatures.

1. **Key Agreement**: Back in 1974, two distinguished mathematicians, Whitfeld Diffie and Martin Hellman, invented the Diffie-Hellman key agreement protocol that uses public key cryptography. In this protocol, two parties can agree on a shared secret key without transmitting the key directly. Instead, they exchange public keys and use a mathematical function to generate the shared secret key. This provides a secure way to establish a shared secret key that can be used for encryption/decryption or other cryptographic purposes.

2. **Digital Signatures**: A digital signature is a way to ensure the authenticity and integrity of a message. To create a digital signature, the sender uses their private key to sign the message. The recipient can then verify the signature using the corresponding public key. If the signature is valid, the recipient can be sure that the message has not been tampered with by an unauthorised third party (eavesdropper) and that it was indeed sent by the sender.

Public key cryptography is a powerful tool for secure communication and is used in various applications, including online banking, e-commerce, and secure messaging.

TLS makes use of the Diffie-Hellman key agreement protocol to generate a shared secret that is used for generating a TLS session key. In ISO 15118, we use what is called a key derivation function to calculate the TLS session key from the shared secret key.

Hash functions for digital signatures

Hash functions are an important component of digital signatures. A hash function is a mathematical function. It takes input data of arbitrary size (like an ISO 15118 message exchanged between EV and charging station) and produces a fixed-size output, known as a hash or a message digest. The output is a unique representation of the input data, which is typically much smaller than the original data. If that sounds a bit too abstract, then maybe have a go at this online hash generator to see how text input is converted to its corresponding hash value.

In digital signatures, a hash function is used to create a fixed-size representation of the message that is being signed. The sender then signs (i.e. encrypts) the hash value using their private key to create the digital signature. The recipient can verify the signature by computing the hash value of the received message. This works by decrypting the encrypted hash value from the sender using the corresponding public key and comparing the calculated hash value to the hash value that was signed by the sender. If the two hash values match, the recipient can be certain that the message has not been tampered with and that it was indeed sent by the sender.

In ISO 15118-2, we use the hash function SHA-256, which means that the hashes are 256 bits long. ISO 15118-20 also makes use of SHA-384.

Using a hash function in digital signatures has several benefits:

1. **Message integrity**: Hash functions ensure that the message has not been tampered with during transmission. Even if a single bit of the message is changed, the hash value will be completely different, making it impossible for the recipient to verify the signature.

2. **Efficiency**: Hash functions can process large amounts of data quickly and efficiently, making them ideal for use in digital signatures.

3. **Confidentiality**: Since the hash value is a fixed size, it does not reveal any information about the original message. This means that the original message can be kept confidential, while the hash value can be used for verification purposes.

Using a hash function in digital signatures provides an efficient and secure way to ensure message integrity and to verify the authenticity of the sender.

The specific case for Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a form of public key cryptography that is especially useful for embedded devices due to its small key sizes, efficient operations, and strong security properties.

Here are some reasons why ECC is particularly well-suited for use in embedded devices that come into play also in EVs and charging stations:

1. **Small key sizes**: ECC uses smaller key sizes compared to other public key cryptography schemes, such as RSA. This is because ECC relies on the mathematical properties of elliptic curves, which allow for smaller key sizes without compromising security. Smaller key sizes result in less storage and processing requirements, which is a critical consideration for embedded devices with limited storage capacities (memory).

2. **Efficient operations**: ECC operations are typically faster and require less processing power than other public key cryptography schemes. This is because the operations in ECC are based on elliptic curve point addition and multiplication, which can be implemented using simple and efficient algorithms. This makes ECC particularly attractive for use in (embedded) devices with limited computing power.

3. **Strong security properties**: Despite its small key sizes and efficient operations, ECC provides strong security properties comparable to other public key cryptography schemes. ECC is based on the discrete logarithm problem on elliptic curves, which is believed to be hard to solve computationally. This means that ECC keys are resistant to attacks from both classical and quantum computers.

Overall, ECC is a good choice for embedded devices like the electronic control units used in EVs and charging stations because it provides strong security with small key sizes and efficient operations, making it a practical solution for devices with limited processing power and memory resources.

ISO 15118-2 demands the use of specific elliptic curve called ‘secp256r1’ (aka ‘prime256v1’) for the following well-established ECC algorithms:

- Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol to generate the TLS session key during the TLS handshake
- Elliptic Curve Digital Signature Algorithm (ECDSA) to generate digital signatures with the private key and to verify digital signatures with the corresponding public key

TLS cipher suites

You've now learned about a set of cryptographic algorithms that are used to secure the communication link between a client and a server, or more specifically, between an EV and a charging station. TLS refers to a particular combination of these algorithms, in particular the following four cryptographic building blocks, as a 'cipher suite'.

1. **Key exchange algorithm**: This is used to establish a shared secret between the client and server. Examples of key exchange algorithms include Diffie-Hellman (DH), Elliptic Curve Diffie-Hellman (ECDH), and RSA.

2. **Authentication algorithm**: This is used to authenticate the identity of the server to the client, and vice versa. Examples of authentication algorithms include RSA, DSA, and ECDSA.

3. **Bulk encryption algorithm**: This is used to encrypt data in transit. Examples of bulk encryption algorithms include AES, Blowfish, and RC4.

4. **Message authentication algorithm**: This is used to verify the integrity of messages and prevent tampering. Examples of message authentication algorithms include HMAC and Secure Hash Algorithm (SHA).

When a TLS connection is established between a client and server, they negotiate which cipher suite to use. The negotiated cipher suite determines the algorithms that will be used for key exchange, authentication, encryption, and message authentication.

The strength of a TLS cipher suite depends on the strength of its individual components. For example, the strength of the bulk encryption algorithm determines how difficult it is for an attacker to decrypt the data in transit. The key exchange algorithm determines the strength of the shared secret, which in turn affects the strength of the encryption.

Overall, the choice of cipher suite has a significant impact on the security of a TLS connection. It is important to choose a cipher suite that provides strong security while also being compatible with the systems being used.

In ISO 15118-2, there are only two cipher suites to choose from:

- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

However, only the latter one facilitates 'Perfect Forward Secrecy' (PFS), which is a desired characteristic in secure communications.

The 'E' in ECDHE stands for 'Ephemeral' and means short lived or temporary. This forces the EV and charging station to create a new and unique temporary private and

public key pair for each new charging session and discard the key pair after the TLS session is terminated. This means if an attacker were to obtain the long-term key used in a Diffie-Hellman key exchange, they would not be able to use that key to decrypt the communications in any previous or future sessions. This is because a new TLS session key is always generated using a different private-public key pair. That's what perfect forward secrecy is all about.

To summarise, each ISO 15118 communication session should only use the following cipher suite, which specifies the particular key agreement algorithm, signature algorithm, and encryption algorithm to use:

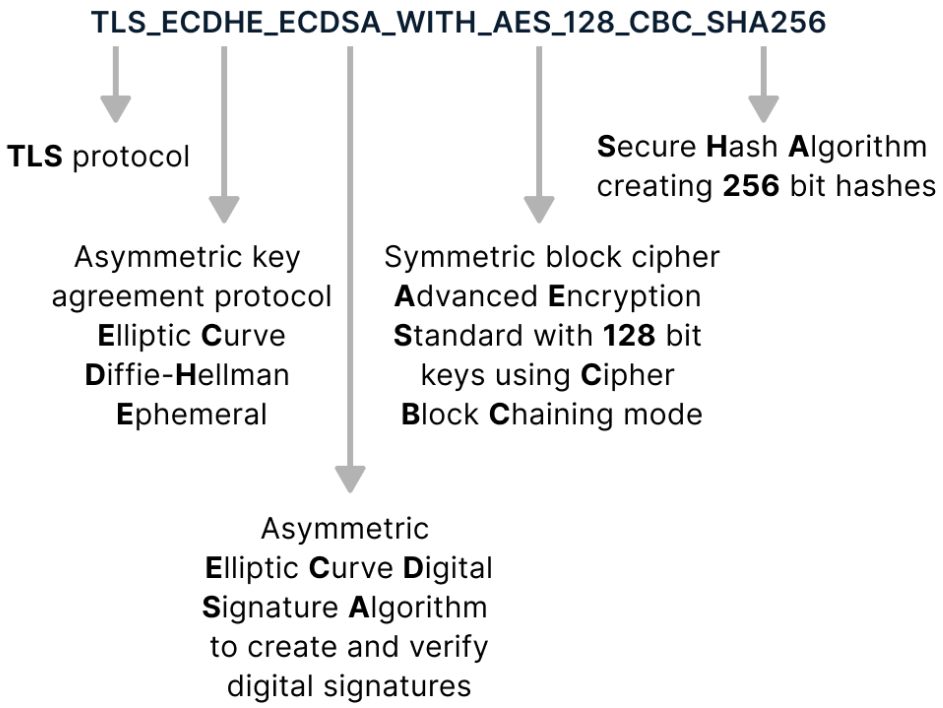

Fig. 1: The components of a TLS cipher suite

ISO 15118-20 proposes a new set of cipher suites to enhance data security and be more resilient against cyberattacks, also taking into account the possibilities that will arise when using quantum computers to do cryptanalysis.

The new cipher suites for ISO 15118-20, which demands the use of TLS 1.3, are:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

In TLS 1.3, the handshake is quicker because the key exchange algorithm is known from the start (ECDHE). That's why it no longer appears in the beginning of the cipher suite name.

Digital certificates

The last topic we need to cover, before we return to where we left off with the Plug & Charge ecosystem and public key infrastructures, are digital certificates.

A digital certificate is a digital document that serves as a form of identification and provides a means of verifying the identity of an individual, organisation, or device. It contains information about the identity of the certificate holder, including their name or a possible serial number and the public key.

Digital certificates are issued by trusted third-party organisations called Certificate Authorities (CAs), which are responsible for verifying the identity of the certificate holder and issuing the certificate. The certificate is signed by the CA using its private key, which allows anyone who has the CA's public key to verify the certificate's authenticity.

Each player outlined above in the section on the Plug & Charge ecosystem is issued their own certificate. One particular certificate I would like to highlight is the Contract Certificate, which identifies the billing account with a Mobility Service Provider (MSP). The Contract Certificate is what the EV presents to the charging station to identify and authorise itself on behalf of the EV driver (or owner) in order to recharge its battery (more on this later when we discuss how a Plug & Charge session works).

Here's an example of a Contract Certificate, which is nothing else than a digital data record in a specific format called X.509.

```
openssl x509 -in contractLeafCert.der -inform DER -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            4b:10:70:4c:9d:37:db:a1:1e:3c:28:85:af:dc:2b:55
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = US, O = Electrify America LLC, CN = US MO Sub2 CA QA G2.2.1
        Validity
            Not Before: Jul 29 14:19:09 2022 GMT
            Not After : Dec 10 11:42:59 2022 GMT
        Subject: O = Hubject Inc, CN = EMP99SWTUSQA001
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:35:46:e1:db:b3:46:89:9e:c8:eb:87:ee:e0:86:
                    27:a7:61:78:8e:dc:20:10:5f:96:49:1c:4f:7d:01:
                    ad:56:1c:a7:db:7b:0a:5f:22:3f:16:bd:61:2c:cc:
                    10:67:c8:75:9c:a1:a5:f1:85:96:2a:fb:37:10:50:
                    d7:33:66:8d:35
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                4E:82:6B:C5:BF:5E:97:F0
            X509v3 Authority Key Identifier:
                keyid:4D:F0:A8:EE:80:94:32:68

            Authority Information Access:
                OCSP - URI:http://ocsp-qa.electrifyamerica.com:8080

    Signature Algorithm: ecdsa-with-SHA256
         30:44:02:20:48:42:59:4c:32:1b:46:72:18:a7:56:c9:98:86:
         07:41:2f:f6:b0:5b:6a:21:e5:15:f2:02:44:63:ab:b3:20:66:
         02:20:34:3d:71:52:ce:5b:de:27:7e:0d:04:df:b8:2f:83:9d:
         96:5e:44:b7:d7:fc:f1:64:62:a0:68:ef:ec:18:f5:d3
```

Fig. 2: Example of a Contract Certificate, issued by a test instance from Hubject

Let me highlight a few of the contents of this certificate. The first line is just the openSSL command you'd have to put in a command line terminal if you wanted to read out the contents of a given certificate. In this case, the certificate is DER-encoded, which is a binary encoding format that must be used for ISO 15118:

- **Serial number**: This is the unique identifier of this certificate within the realm of the issuing Certificate Authority (CA). No two certificates issued by the same CA have the same serial number.

- **Signature algorithm**: This is the algorithm the issuing certificate authority used to digitally sign this certificate with its private key. As you can see, the Elliptic Curve Digital Signature Algorithm in combination with the Secure Hash Algorithm producing 256-bit hashes comes into play. To verify the signature of this certificate, one must get hold of the digital certificate of this issuing CA.

- **Issuer**: This is the organisation acting as a CA who issued this certificate. In this particular case, it is US-based Electrify America. The 'MO Sub2' stands for 'Mobility Operator Sub Certificate Authority 2'. In ISO 15118, we use the term Mobility Operator (MO), which is a synonym for Mobility Service Provider (MSP). We'll touch upon the Sub2 when we discuss certificate hierarchies in the context of PKIs. The 'QA' stands for 'quality assurance', which means this is a test certificate issued for a testing environment.

- **Validity**: A certificate has a clearly defined validity period. It can be issued to become valid instantly or in the near future. It also has to expire at some point according to the certificate policy the CA is operating under.

- **Subject**: This field identifies the entity that the certificate is issued for. It typically includes the common name (CN) and the fully qualified domain name (FQDN) of the entity, which are used to identify the server or system that the certificate is associated with. However, in the ISO 15118 use case, the CN field of a contract certificate reflects the E-Mobility Account Identifier, or EMAID. This is the billing account towards which the energy is billed that is used to recharge an EV's battery. The 'O' stands for Organisation and illustrates that Electrify America is using Hubject's service to issue Contract Certificates.

- **Subject Public Key Info**: Here you can see that the public key is an elliptic curve (EC) public key that is 256 bit long. It has been created using the prime256v1 elliptic curve I mentioned in the section on elliptic curve cryptography.

- **Authority Information Access**: This part of the X.509 extensions contains the URL of the OCSP responder. OCSP stands for Online Certificate Status Protocol and is a fast responding web service that tells you whether or not a certificate has been revoked. Certificates need to be constantly checked for revocation. Reasons for revoking a certificate can be a compromised private key or a CA changing its name.

- **Signature Algorithm**: The issuing CA's signature itself is the last entry of a certificate.

Now you should have a fairly good understanding of the various data security mechanisms in place to enable confidentiality, data integrity and authenticity between the EV and the charging station.

Cryptography is no easy fare. But I hope I was able to shed some light on it and demystify this complex topic for you.

This cryptography section only focused on how to secure the communication between the EV and the charging station. But we also need to make sure the charging station and the cloud-based backend, or Charging Station Management System (CSMS), are exchanging information in a secure way.

Luckily, the data security principles that apply to the EV and charging station are pretty much the same for the charging station and its backend. The only major difference is the certificates that are being used. That's why we should now shift our focus towards the relevant Public Key Infrastructure, or PKI, that needs to be in place for the Plug & Charge magic to happen.

Public Key Infrastructure for Plug & Charge

ISO 15118 operates inside a Public Key Infrastructure (PKI) ecosystem. A PKI is a system of technologies, certificate policies and related audit requirements as well as procedures used to manage and distribute digital certificates and public keys. The main purpose of a PKI is to establish and maintain secure communication between the participants within an ecosystem.

In a PKI system, a trusted third-party called a Certificate Authority (CA) issues digital certificates that contain public keys and other identifying information about the certificate holder. The CA is responsible for validating the digital identity of a certificate holder before issuing the corresponding certificate. This includes managing the creation, storage, distribution, and revocation of digital certificates. It digitally signs the certificate using its own private key, which validates the authenticity of the certificate. To verify this digital signature, one needs to get hold of the public key of the issuing CA, which is stored in the issuing CA's certificate. This establishes a chain of trust, beginning with the so-called end-entity certificate, or leaf certificate. It ends in the root CA certificate, also known as the trust anchor. You can see how computer scientists like to take analogies from nature as we're talking about a tree-like chain of trust from the root all the way to its leaves.

Within the EV charging space, the main participants of the Plug & Charge ecosystem are:

- The electric vehicle (EV)
- The EV manufacturer (here: OEM)
- The charging station
- The Charge Point Operator (CPO)
- The Mobility Service Provider (MSP)
- The Certificate Provisioning Service (CPS)
- The operator of the V2G Root CA
- The operator(s) of the necessary data pools and cloud-based services that need to be in place to facilitate the provisioning of certificates to enable Plug & Charge

A cooperation between all these stakeholders from different industries and geographic locations is key for a successful rollout of a seamless charging experience – no matter which operator or location a driver chooses to charge their EV.

Remember that ISO 15118 focuses solely on the communication between the primary actors, the EV and charging station. Whatever happens behind the charger, including cloud-based backend systems and the PKI ecosystem for Plug & Charge that are referred to as "secondary actors (SA)" in the specification, is out of scope of ISO 15118. Instead, ISO 15118 only sets some minimum constraints to secure the communication between the EV and the charger (using TLS) and to enable Plug &

Charge. A framework for a certificate structure is laid out in ISO 15118, but the implementation of a certificate policy and operational requirements for such a PKI are not defined in ISO 15118. To fill that void, we need to look at the application rule VDE-AR-E 2802-100-1. But we'll get to that in a bit. First, let's look at the resulting certificate framework that you'll find in ISO 15118.

With the ISO 15118 PKI, or V2G PKI as it is also referred to, each member of the Plug & Charge ecosystem can generate specific Root CA certificates, Sub CA certificates, and leaf certificates that are bound to their role in the ecosystem. The V2G Root CA is the highest trust anchor and is necessary to issue the Sub CA and leaf certificates for a CPO and for a CPS[2]. We'll talk about the organisations that offer V2G Root CA (and Sub CA) services in the chapter on current ecosystem providers. An MO Root CA can be created individually by a Mobility Operator ("ISO 15118 speak" for MSP) and similarly, an OEM Root CA can be created by a car manufacturer. Only MSPs and car manufacturers can operate their own root CA if they deem it necessary and useful. They can also opt to use the existing V2G Root CA. The CPO and CPS, on the other hand, need to use the service of a V2G Root CA to issue their Sub CA certificates. The Sub CA are used to issue leaf certificates that are used for different purposes as defined in the ISO 15118 standard and VDE application rule.

A Sub CA basically decouples the need to issue leaf certificates from the root CA, and it is good security practice to keep a root CA offline for most of the time. ISO 15118 demands the use of at least one Sub CA and allows up to two Sub CAs. Some organisations might see the need for two Sub CAs, but I assume in most cases we'll see only one Sub CA.

There is also a concept for a Private Environment (PE), which refers to chargers that are not publicly available, such as in a fleet depot charging environment. The PE has lower security requirements and doesn't foresee a Contract Certificate or any Sub CAs (at least not in ISO 15118-2, in ISO 15118-20 Sub CAs were introduced for PEs). We'll not cover the private environment scenario in this white paper.

Below, you'll find two images: the first one illustrates the proposed certificate structure for ISO 15118-2, the second one for ISO 15118-20. You'll see that they are very similar, with slight changes for Part 20 to enhance security.

[2] I'll explain why we need a Certificate Provisioning Service (CPS) later on when we discuss how the MSP prepares a Contract Certificate to be installed onto the EV.

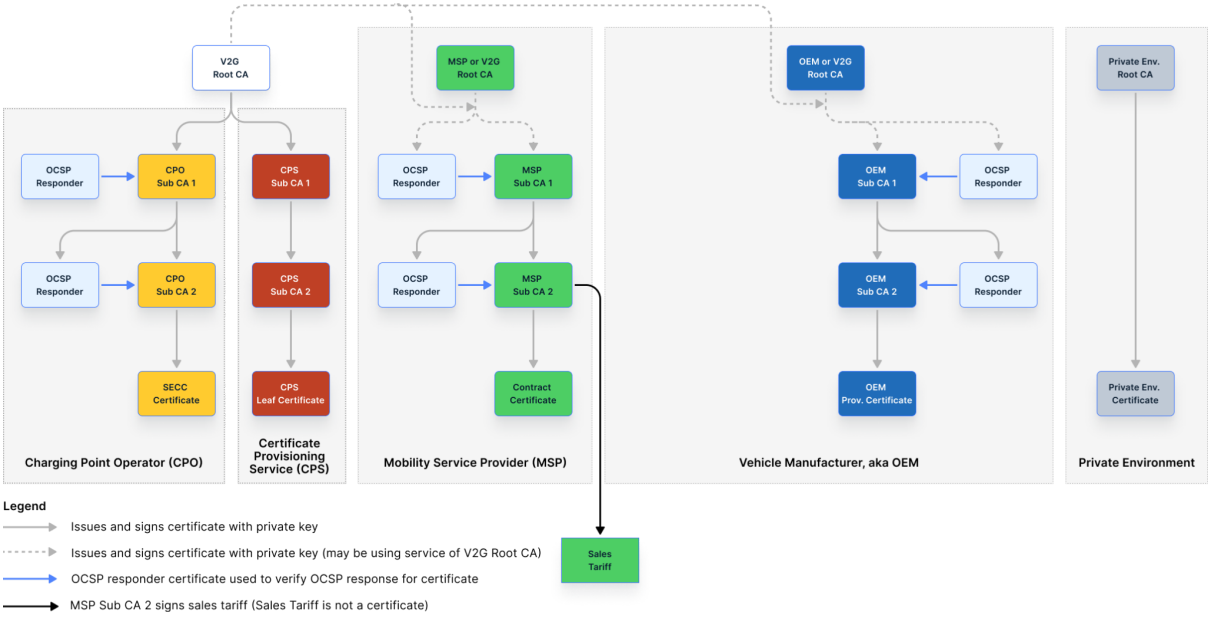

Fig.3: Certificate structure for the ISO 15118-2 PKI

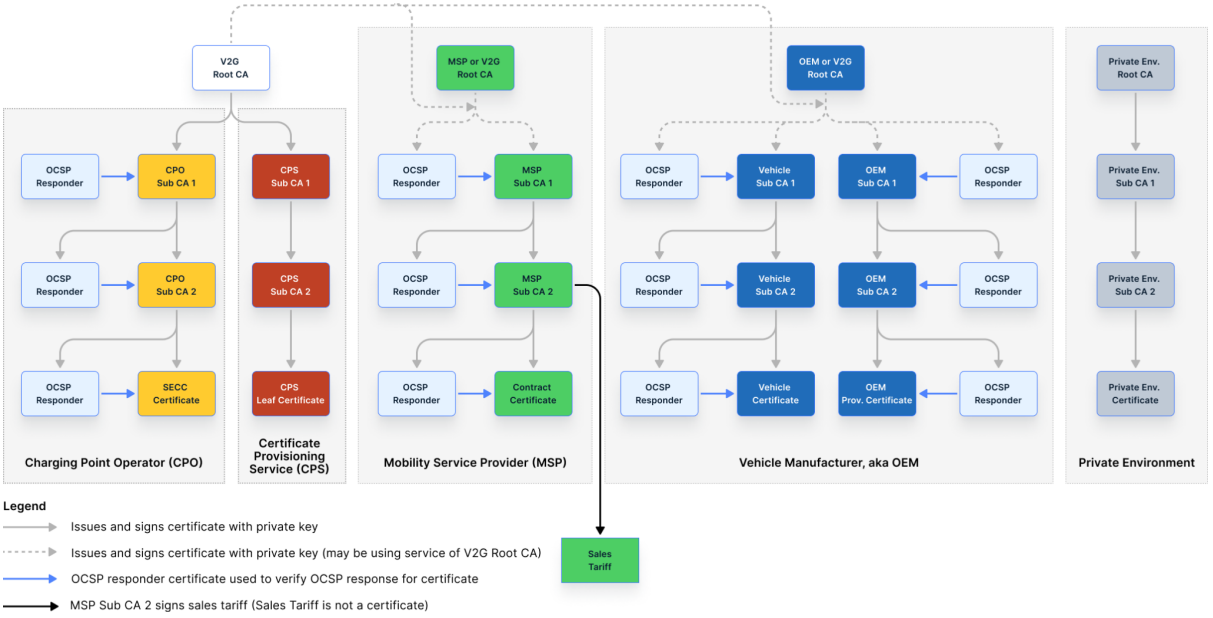

Fig. 4: Certificate structure for the ISO 15118-20 PKI

Now that you have a rough idea of the V2G PKI and its relevant certificates, we've set the foundation to discuss how a Contract Certificate (the leaf certificate in the MSP certificate chain) is being created and installed into an EV.

The next chapter will guide you through these steps as they are outlined in the application rule VDE-AR-E 2802-100-1, which describes all the processes and data pools necessary to provision a Contract Certificate.

Provisioning a Contract Certificate to an EV

The whole process of issuing a contract certificate for a specific EV to enable it for Plug & Charge involves many stakeholders and is divided into several steps. I'm providing you here with a succinct overview, detailed enough to understand the overall process but without going down into any rabbit holes. After all, the point of this white paper is to get a better understanding of the Plug & Charge ecosystem in general.

You can essentially divide the whole process into four steps:

1. Vehicle manufacturer (OEM) prepares an EV for Plug & Charge
2. EV driver signs up for Plug & Charge with an MSP
3. MSP prepares a Contract Certificate for a specific EV
4. Installing the Contract Certificate in an EV

The following subsections will address each step in more detail. You'll find an illustration at the end of this chapter that you might want to keep handy. It will help you to mentally connect the different steps.

Step 1: Vehicle manufacturer (OEM) prepares an EV for Plug & Charge

What does it take to enable an EV for Plug & Charge? Well, it basically comes down to two prerequisites:

1. Establish the grounds for a digital certificate, which is tied to a billing account, to be installed in the EV. This way, the EV can authorise itself automatically for charging as soon as the cable is plugged[3] and the delivered energy can be billed towards the associated billing account from an MSP. We call the digital certificate that is tied to the billing account a 'Contract Certificate'. The certificate used to initiate the provisioning of this Contract Certificate is called the 'OEM Provisioning Certificate'.

2. Make sure the EV can identify a charging station as being trustworthy so that a digitally secured and encrypted communication can be set up. A so-called 'trust anchor' in the form of a digital certificate needs to be in place for this to happen. We call this trust anchor the 'V2G Root CA Certificate'.

[3] For the avoidance of doubt: Plug & Charge is not restricted to manual conductive charging. It also works for wireless charging, pantograph charging (ACD-P) and any other energy transfer service that is already or will soon be specified in ISO 15118, like Automated Conductive Device for Side Coupling (ACD-S) or Automated Conductive Device for Underbody Coupling (ACD-U). We'll still stick with the established term 'Plug & Charge', even though you wouldn't always 'plug in' the cable (yourself).

The OEM Provisioning Certificate

Each EV needs to have a unique identifier so we can assign a billing account to this vehicle. In ISO 15118, this identifier is called Provisioning Certificate ID, or PCID. Its structure is similar to a Vehicle Identification Number (VIN), although it's up to each car manufacturer whether or not to use the VIN as the PCID. This identifier better be digitally secured so it can't be manipulated, which is why we need a digital certificate that includes the OEM's digital signature to prove the authenticity of each PCID. This digital certificate is what we call the OEM Provisioning Certificate in ISO 15118. The 'Provisioning' part in the certificate's name comes from the fact that it is used to install, or *provision*, a Contract Certificate into the EV.

Remember that a digital certificate holds a public key and that the associated private key needs to be stored securely. In the case of the car OEM, that public-private key pair needs to be generated inside the EV. The EV needs to securely store that private key, ideally using a hardware security module that is based on the Trusted Platform Module (TPM)[4] architecture.

Now, if the EV wants to request the installation of a new Contract Certificate via a charging station, it needs to have the OEM Provisioning Certificate already installed and ready to present to the charger. That means that the car OEM needs to make sure the EV is already equipped with an OEM Provisioning Certificate before it gets sold to a customer.

On the other hand, if a car OEM wants to be more in control of the installation process of a Contract Certificate and only allow such installation via their own telematics backend – a trend I see more and more among car manufacturers – the OEM Provisioning Certificate still needs to be created, but not installed on the vehicle itself. Instead, the car OEM only has to make sure the OEM Provisioning Certificate is stored in what we call the Provisioning Certificate Pool. More on that in Step 3.

The Contract Certificate

The Contract Certificate is the secure, digital representation of the billing account towards which all the energy that your EV will charge over time will be billed. This is based on an electricity contract offered by a Mobility Service Provider of your choice, similar to an electricity contract you sign up for at home. I showed you an example of a Contract Certificate when we covered digital certificates, and we'll talk more about it in Step 3.

[4] Trusted Platform Module (TPM) is an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys. The term can also refer to a chip conforming to the standard. More info on the website of the Trusted Computing Group.

The V2G Root CA Certificate

Now, as to the second step listed above, we do need to install a trust anchor into the EV. The principle behind this is similar to the way your web browser is working. What happens in the background is that the https-secured web server is sending your browser a couple of certificates identifying that website as a trustworthy source. With the help of so-called 'trust anchors' – i.e. root CA certificates verified by your browser vendor (like Google Chrome, Apple Safari, Mozilla Firefox) that come pre-configured with the browser – your browser is able to verify the chain of certificate signatures all the way to the verified root CA certificate[5].

To map this browser analogy to the EV charging world: The charging station is the server, the EV is the client, and the list of verified trust anchors is the list of V2G Root CA Certificates.

All root CA certificates in this PKI ecosystem need to be accessible through what is called a Root Certificate Pool, or RCP, to which each member of the V2G PKI ecosystem needs to have authenticated access.

Alright, let's summarise the action points on the vehicle OEM's side for each EV:

1. Install one or more V2G Root CA Certificates (trust anchors) in the EV.

2. Generate a unique Provisioning Certificate ID (PCID) for the EV.

3. Have the EV generate a public-private key pair and store the private key safely inside the EV, ideally using a TPM.

4. Issue and digitally sign an OEM Provisioning Certificate based on the generated public key and the PCID.

5. Store that OEM Provisioning Certificate in the EV (if Contract Certificate installation shall be enabled via the charging infrastructure) and inside the Provisioning Certificate Pool (PCP). The PCP must also hold the info about the supported ISO 15118 protocol versions and the installed trust anchors (V2G Root CA certificates).

6. (If the EV is to be used in a Private Environment (PE) and a PE Root CA certificate is available, then store this on the EV as well).

[5] See the section on Public Key Infrastructure for Plug & Charge to better understand what a 'root CA' certificate and certificate chains are.

Step 2: EV driver signs up for Plug & Charge with an MSP

The EV driver, or owner, needs to sign up for an EV-specific electricity contract offered by a Mobility Service Provider. How that sign-up process works is out of scope of ISO 15118, that's completely up to each MSP.

The process will likely be similar to choosing an electricity provider for your home, except that you'll need two additional pieces of information:

1. The PCID that uniquely identifies your EV

2. A vehicle registration document that proves that you're the rightful owner of that EV

How the EV driver gets access to that PCID is also completely up to the car OEM. This could be a document handed out upon purchasing the vehicle, or it could be accessible via the OEM's app, for example. Alternatively, this signup process might be just as simple as ticking a box when purchasing a vehicle as over time pretty much every car manufacturer will offer an MSP solution themselves. This streamlines the process for their customers and helps them expand the value chain of their offerings. This adds to the seamlessness of the user journey, but it needs to happen in a non-discriminating way, more on that in a chapter on market governance rules.

That's it, basically. This then triggers the procedure outlined in Step 3.

Step 3: MSP prepares a Contract Certificate for provisioning

The Mobility Service Provider's job is to offer you an electricity contract with one or more associated billing accounts (for you and your family, or for each EV in your fleet business), and to enable your EVs for Plug & Charge. To do so, we need a billing account ID and the associated digital certificate.

In the land of ISO 15118, we refer to the billing account ID as the EMAID, which is short for E-Mobility Account ID, and the associated digital certificate is the aforementioned Contract Certificate. The EMAID has a clearly defined syntax that is specified in Annex H of ISO 15118-2:

E-Mobility Account ID (EMAID) =

1. **Country code**: Two-letter country code (e.g. 'GB' for Great Britain)
2. **Optional separator**: Hyphen as an optional separator ('-')
3. **Provider ID**: Three alphanumeric characters, uniquely identifying the MSP (e.g. 'SEV' for Switch EV)
4. **Optional separator**: Hyphen as an optional separator ('-')
5. **E-mobility Account Instance**: Nine alphanumeric characters, uniquely identifying the billing account (e.g. 'C12345678')

6. **Optional separator**: Hyphen as an optional separator ('-')
7. **Optional check digit**: A single check digit, optional but recommended. See Annex H.1.3 in ISO 15118-2 for its computation.

The EMAID is case insensitive, which means that 'GBSEVC123456780' would be the same EMAID as 'gbsevc123456780'. The optional separator can be used when communicating an EMAID to users for better legibility and typing.

Next step is to create the Contract Certificate itself and make the associated private key available to the EV in such a way that only the EV is able to read that private key.

But first, the MSP needs to create a new public-private key pair. It'll then issue and digitally sign the Contract Certificate based on that public key and the freshly generated EMAID. Finally, the MSP needs to encrypt that private key for the EV that is uniquely identified by the PCID that the EV driver has submitted to the MSP when signing up for the electricity contract. It may sound like a mouthful, so let's summarise the necessary steps in slightly more detail.

1. Create an E-Mobility Account ID (EMAID, the billing account) that is associated with exactly one electricity contract and exactly one EV. The EMAID-to-EV association happens via the unique PCID that the EV owner provided when signing up for the electricity contact.

2. Request the OEM Provisioning Certificate (and the associated information like OEM Sub-CA Certificates, the supported ISO 15118 protocols and trust anchors installed in the EV) from the car manufacturer's Provisioning Certificate Pool, using the PCID provided by the EV driver. In case of a deeper integration between car manufacturer and MSP, that PCID might even have been provided by the car manufacturer itself.

3. Request the OEM's Root CA Certificate (could be the V2G Root CA Certificate or a dedicated OEM Root CA Certificate) from the Root Certificate Pool to verify the authenticity of the OEM Provisioning Certificate. Also check that each of the certificates from the car OEM is still valid and has not been revoked.

4. Create a public-private key pair and have the MO Sub CA 2[6] issue the Contract Certificate based on that public key and the EMAID.

5. Encrypt the freshly generated private key so that only the EV, to which the PCID refers, is able to decrypt and use it. To do so, the MSP needs the OEM Provisioning Certificate's public key. I'll spare you the details of how this private

[6] If you don't know what an MO Sub CA 2 is, then you might want to jump back to the Public Key Infrastructure for Plug & Charge chapter to learn more.

key is being encrypted and rather refer to the ISO 15118 Advanced Training[7]. Once the private key is encrypted, the MSP needs to delete the unencrypted copy of the private key, thereby following good cybersecurity practices (a private key shall never exist in more than one place and only be accessible by the party that is supposed to use that private key).

6. Assemble several bits of information into a Contract Certificate Bundle (CCB), consisting of:
    a. the Contract Certificate,
    b. associated Sub CA certificate(s),
    c. the encrypted private key,
    d. the EMAID,
    e. the PCID,
    f. information about the supported ISO 15118 versions of the EV,
    g. information about the V2G Root CA Certificates installed in the EV, and
    h. Information relevant for the EV to decrypt the private key (also known as Diffie-Hellman public key)

7. Send this Contract Certificate Bundle to a Certificate Provisioning Service

The role of the Certificate Provisioning Service

The Certificate Provisioning Service's job is to verify the authenticity of the MSP's Contract Certificate chain and to prepare a digitally signed Certificate Installation Response. The Certificate Installation Response is an ISO 15118 message that the charging station needs to send to the EV in response to the EV's Certificate Installation Request. The EV uses this message only if it intends to authorise for charging via Plug & Charge, but does not have a valid Contract Certificate installed and asks the charging station to install it.

The CPS needs to store that digitally signed Certificate Installation Response, together with some other pieces of information, in another data pool, called the Contract Certificate Pool, or CCP. It may seem a bit excessive with all these abbreviations. To provide a better overview, I've included an abbreviation cheat sheet at the end of this white paper for a better overview.

There are a few additional intricate steps involved for the CPS, but unless you're an organisation like Hubject or CharIN that operates Plug & Charge services for MSPs, OEMs and CPOs, you don't need to be concerned about them.

One note on the necessity of the CPS: In deregulated markets like Europe, the CPO and MSP must be separate legal entities. In order for the EV to verify the authenticity

[7] See dates and registration details for the upcoming 'Charging Communication with ISO 15118' training on the CharIN Academy website.

of the Contract Certificate, it needs to have the relevant root CA certificate aka trust anchor installed. The challenge now lies in the fact that, according to ISO 15118, an MSP has the freedom to operate an MSP Root CA of their own instead of using the services of a V2G Root CA. This would result in the potential need for EV manufacturers to install all kinds of MSP Root CA Certificates as trust anchors, which is a potential nightmare for the cost-sensitive automobile industry that wants to reduce the costs for storing digital certificates to an absolute minimum. Instead, the role of a Certificate Provisioning Service was created. The CPS should instead verify the authenticity of the MSP's Contract Certificate and be mandated to issue its own certificates from a V2G Root CA whose trust anchor certificates are already installed in the EV. The principle behind this is that of transitive trust: The EV trusts the CPS, the CPS trusts the MSP, therefore the EV can trust the MSP (and its Contract Certificates).

Now, in other markets like the US, we don't see the same level of deregulation (yet). This means that the CPO could be the same entity as the MSP. One example is Electrify America, a company that is both operating charging infrastructure and offering MSP services for Plug & Charge. Strictly speaking, in this case you may not need the CPS and instead directly link the MSP to the Contract Certificate Pool.

Step 4: Installing a Contract Certificate in an EV

The Contract Certificate Pool's (CCP) main purpose is to enable the delivery of Contract Certificates and precompiled Certificate Installation Responses as quickly as possible to the EV. At the same time, the CCP also needs to validate the incoming requests and make sure the stored data (i.e. Contract Certificates and all data contained in the Contract Certificate Bundles) is still valid and not expired.

There are actually two ways to install a Contract Certificate in an EV which I already mentioned briefly in this white paper: Alternative A is via the car OEM's telematics backend, alternative B is via the charging infrastructure.

Alternative A: Installing a Contract Certificate via the car OEM's telematics backend

If a car manufacturer supports the installation of a Contract Certificate via an over-the-air (OTA) update using its telematics backend, the car OEM would need to register with the Contract Certificate Pool to get notified instantly of any updates. Think of it as a publish-subscribe mechanism: The car OEM subscribes to any updates for Contract Certificates. The Contract Certificate Pool publishes these updates the second a new Contract Certificate is being installed in the CCP and forwards the certificate to the car OEM backend. This is becoming the go-to solution for an increasing number of EV manufacturers as it allows them to be in control of the installation process and the user journey when selecting the right Contract Certificate for Plug & Charge sessions. See also the section on market governance rules, which reflects on the freedom of choice for EV drivers to select an MSP contract.

For this scenario, we wouldn't really need the Certificate Provisioning Service, as the cloud-based car OEM backend can take care of all the validation and verification the CPS would usually do and directly install the Contract Certificate and associated encrypted private key into the EV. The EV then doesn’t need to process a Certificate Installation Response but only needs to decrypt the encrypted private key and safely store the private key alongside the Contract Certificate.

Alternative B: Installing a Contract Certificate via the charging infrastructure

Installing a Contract Certificate via the charging infrastructure involves a few more steps that need to be carefully orchestrated and tested to make sure the Plug & Charge experience is as smooth as possible:

1. The EV is plugged into the charging station. It is configured to do Plug & Charge, and realises the need to install a Contract Certificate as no valid Contract Certificate is currently installed.

2. The EV sends a Certificate Installation Request message (as part of the ISO 15118 message sequence) to the charging station. This message is encoded in a specific format which is called EXI (Efficient XML Interchange). The encoding result is a binary representation of the message, which is significantly smaller than the original ISO 15118 message itself. It can be processed more efficiently on the communication controllers of an EV or a charging station.

3. The charging station decodes the EXI encoded Certificate Installation Request to be able to read and process the message content. It will then realise that it needs to forward this message to the CPO backend. The Open Charge Point Protocol (OCPP) version 2.0.1 has been designed to enable ISO 15118 Plug & Charge and provides a message called ‘Get15118EVCertificateRequest’. The charger then encodes the Certificate Installation Request (ISO 15118) message in EXI format again. It forwards this message to the CPO backend using the Get15118EVCertificateRequest (OCPP 2.0.1) message. Note that the web service-based OCPP protocol cannot transmit binary (EXI encoded) message content. Therefore, the charger needs to apply Base64 encoding to the EXI encoded message to send this payload with a Get15118EVCertificateRequest message to the CPO backend (aka the CSMS).

4. The CPO backend merely acts as a gateway and forwards the Base64 and EXI encoded Certificate Installation Request to the Contract Certificate Pool, along with the information about the ISO 15118 version(s) supported by the EV (that info is also part of the Get15118EVCertificateRequest message).

5. The Contract Certificate Pool verifies the EV's request and checks whether a valid Certificate Installation Response is currently stored in its database that belongs to this EV. If such data exists, the CCP returns the Base64 and EXI encoded Certificate Installation Response to the CPO backend.

6. The CPO, again acting as a gateway and not processing the content of the received data, directly forwards this data to the charging station using the 'Get15118EVCertificateResponse'.

7. The charging station removes the Base64 encoding and responds to the EV with the still EXI encoded Certificate Installation Response message.

8. Remember that both the encrypted private key, that is associated with the Contract Certificate's public key, and the Contract Certificate itself, are part of the Certificate Installation Response. The EV then decodes this message, verifies the authenticity of the message's signature, decrypts the private key, and safely stores the private key alongside the Contract Certificate.

Now, the EV has everything in place to start the charging process via Plug & Charge, which we'll cover step by step in the next chapter.

It's important to note that we only have five seconds for this installation path as ISO 15118 defines a 5 second timeout for the certificate installation procedure. This means that as a CPO you better make sure that the chargers you manage have a fast and reliable internet connection. Use an Ethernet connection wherever possible, and a reliable 4G or 5G cellular network in cases where no Ethernet connection is possible.

All right, there you have it. This is the lay of the land when it comes to provisioning a Contract Certificate for an EV. As you can see, whereas the CPO has the easiest job in this process, the car OEM and MSP are more intricately involved.

Here's a visual summary illustrating how the various market roles interact. As you read through this chapter (you may want to reread it, it's not an easy fare), I recommend printing out this graphic or enlarging it on a separate screen. It will help you to mentally connect the different steps.

Please note, the Contract Certificate, OEM Provisioning Certificate and SECC Certificate in this image actually represent certificate chains, i.e. the leaf certificate itself and its associated Sub CA certificate(s). To make this clear, I have visualised this by positioning two certificates behind each other.

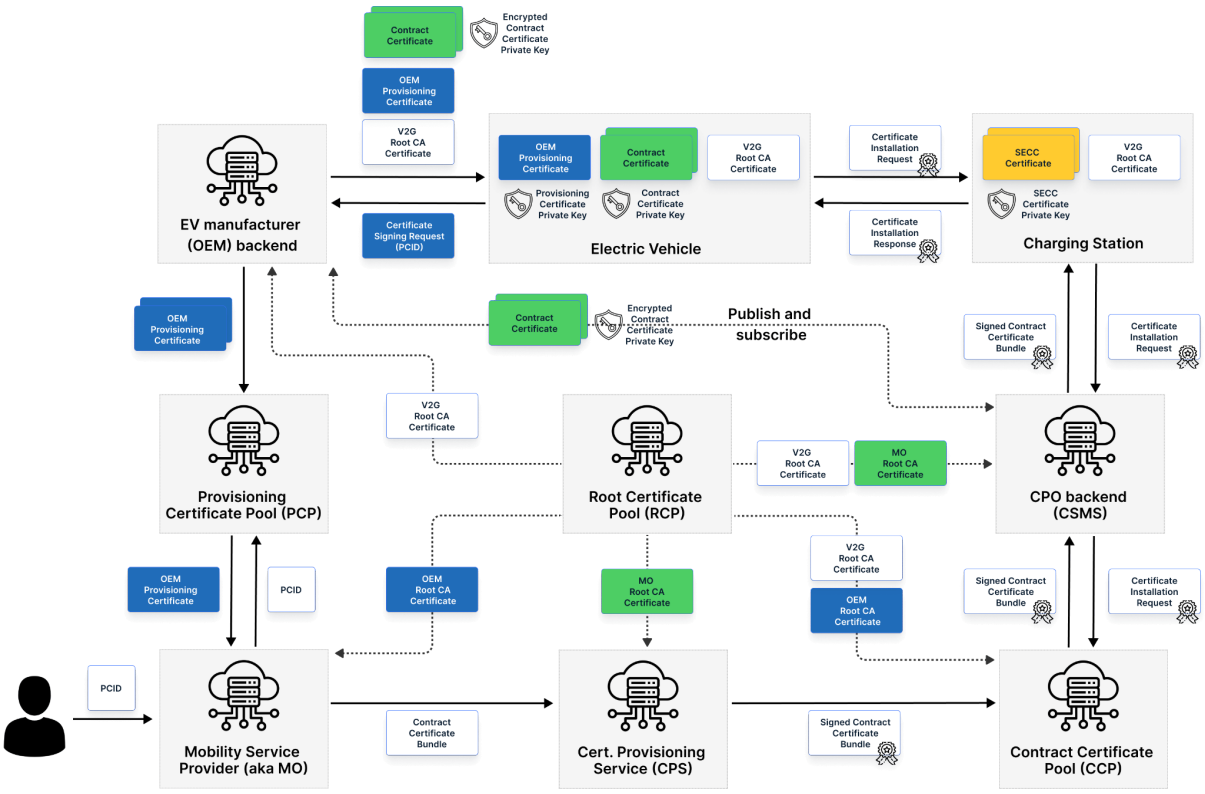

Fig. 5: V2G PKI ecosystem for provisioning of a Contract Certificate to the EV (based on ISO 15118-2)

How a Plug & Charge session works

The previous section focused on the whole orchestra of processes and communication links between the car manufacturer, MSP, CPO and other services within the V2G PKI ecosystem to create a Contract Certificate and get it installed in an EV. Now that we've covered the provisioning of a Contract Certificate, let's discuss the steps needed to successfully run a Plug & Charge session.

It essentially boils down to the following three steps, which we'll dive deeper into one by one.

1. Set up a secure communication link between EV and charger
2. Offer and select Plug & Charge as a means of identification
3. Present the Contract Certificate to the charger and verify its authenticity

Step 1: Set up a secure communication link between EV and charger

Just to be clear upfront: I'll abstract some of the details on how the EV and charger set up a communication link, which starts with a 5% PWM (Pulse Width Modulation) signal and the HomePlug Green PHY-based SLAC (Signal Level Attenuation Characterisation) protocol. If you're interested in these details, please head over to the CharIN Academy website to check when the next "Charging Communication with ISO 15118" Basic training will take place. I'll also dive deeper into the various steps of a TLS handshake during the Advanced training, which usually takes place the week after the Basic training.

Alright, let's focus on how the TLS handshake works on a high level. We already established in Step 1 of the provisioning process that the EV needs to have the same trust anchor installed that the Charge Point Operator (CPO) is using to issue the certificates for its chargers under management – otherwise the EV will not be able to verify the authenticity of the SECC Certificate chain from the charging station. Remember the browser analogy? It's the same principle.

At the start, the EV and charger agree on the TLS protocol to use: TLS 1.2 is mandated for ISO 15118-2; TLS 1.3 is mandated for ISO 15118-20. With different ISO 15118 versions come different required cipher suites and crypto algorithms, which means we also have different certificates that apply (based on these crypto algorithms). Please make sure to create and use digital certificates that adhere to the certificate profiles specified in the corresponding ISO 15118 version (see Annex F in ISO 15118-2 and Annex B in ISO 15118-20).

The charging station will send its SECC Certificate[8] together with its CPO Sub CA Certificate(s) to the EV to authenticate itself towards the EV as a trustworthy charger. The EV then uses its pre-installed V2G Root CA Certificate – the trust anchor – to verify the authenticity by checking all the signatures from the SECC Certificate all the way up the chain to the V2G Root CA Certificate.

The EV also needs to check that none of the certificates have expired or been revoked. The revocation status can be checked using the Online Certificate Status Protocol (OCSP). The certificate authority that issues a certificate usually also operates a so-called 'OCSP responder', which is a fast responding web service that informs about the revocation status of a specific certificate. TLS includes a useful feature called 'OCSP stapling', which allows the charger to add the OCSP response to the TLS handshake. This alleviates the need for the EV to retrieve an OCSP response through a separate web service connection.

There's a slight difference between ISO 15118-2 and -20 regarding the revocation check. While ISO 15118-2 uses so-called 'fast expiring' SECC Certificates that have to be renewed every three months, ISO 15118-20 demands the use of OCSP for both the CPO Sub CA Certificate(s) and the SECC Certificate.

That's basically it. Once the EV has successfully verified the authenticity of the charger, all subsequent communication is digitally encrypted.

Step 2: Offer and select Plug & Charge as a means of identification

There's a clearly defined message sequence the EV and charger need to exchange to make an ISO 15118 based charging session a success. Among those messages is an agreement on the identification method to be used. ISO 15118 specifies two methods:

1. External Identification Means (EIM): This is basically any form of identification that does not involve Plug & Charge, like RFID cards, credit cards, QR code or app-based authorisations.

2. Plug & Charge (PnC): This is the most user-convenient way to start a charging session, just plug in the cable and let the EV do the rest for you.

[8] ISO 15118-2 refers to this certificate as the 'EVSE Leaf Certificate'. But this term is actually not precise enough as we only need a digital certificate per communication device (the Supply Equipment Communication Controller, or SECC) in a charging station, and not one per Electric Vehicle Supply Equipment, or EVSE, that supplies power to the outlets. We can control several EVSEs with a single SECC. You don't need to create a certificate per EVSE, only if you have a 1-to-1 relationship between SECC and EVSE in your charging station setup. The new wording 'SECC Certificate' has been adopted in ISO 15118-20 to reflect this more precise view.

Now, here's where it can get a bit tricky if you don't implement things the right way. It's important that you don't try to identify the EV driver twice. How could that happen you ask? Well, consider the following scenario:

1. A driver arrives at a charging station and uses an RFID card or app first to authenticate himself or herself for the charging session.

2. The driver THEN plugs in the charging cable.

3. If the charger still offers both ways of identification and the EV has Plug & Charge configured as its default identification mechanism, it may identify the EV driver twice. In the worst-case it might even double charge them on different accounts. That only causes confusion on the driver's side, and you'll end up with an angry customer who got charged twice for the same charging session.

Instead, be smart and make sure that your charging station software doesn't offer Plug & Charge once the user has already used the EIM identification method. If, however, Plug & Charge fails for whatever reason (e.g. due to an expired or invalid Contract Certificate), it's advisable to offer EIM as a fallback solution.

Best practice for offering both Plug & Charge and EIM

One way to go about implementing a graceful degradation (first Plug & Charge, then EIM) would be my following suggestion:

1. If the EV driver successfully identifies themselves using EIM before plugging in the cable, don't offer Plug & Charge.

2. If the EV driver first plugs in the cable, then offer both EIM and Plug & Charge.

3. If Plug & Charge identification is successful, you're good. If the Plug & Charge identification fails because the presented Contract Certificate expired or is not allowed at this CPO's charging station network, terminate and trigger a reset of the communication session[9]. Once the EV initiates the ISO 15118 communication anew, offer both EIM and Plug & Charge again to allow the EV to either use another, already installed Contract Certificate[10] or to trigger an installation of a new Contract Certificate via the charging station (if the

[9] You can use the analog PWM signal to trick the EV into 'believing' that the cable was plugged out and in again, which should trigger the EV to re-initiate the SLAC protocol to set up the communication link. Unfortunately, not every EV seems to behave the same way and CharIN has yet to come up with an interoperability guide on how to avoid a plug out and plug in event for the EV driver in case of a failed charging session.
[10] BMW was the first to announce support for 'Multi-Contract Plug & Charge'. It's only a question of time when other car OEMs will follow.

charging station has implemented this feature). The installation process happens before the EV tries to identify itself.

4. If the new Plug & Charge identification with the new Contract Certificate works, you're good. If not, terminate the communication session and trigger another reset. This time, you may only offer EIM to avoid an infinite loop of frustrating Plug & Charge identification attempts.

In any case, it's advisable to keep the EV driver informed with relevant information about the identification progress on the charger's display, if it is equipped with one.

Multi-contract handling with ISO 15118-20

ISO 15118-20 offers a more refined way of handling multiple Contract Certificates, both in terms of allowing the installation of multiple Contract Certificates at once and in terms of switching between various installed Contract Certificates during an ongoing charging session. Thanks to the introduction of additional WARNING error codes in ISO 15118-20 instead of only FAILED error codes (ISO 15118-2), we can trigger the EV to retry a certain action instead of terminating the communication session.

Here's how multi-contract handling works with ISO 15118-20 when choosing the right Contract Certificate for a charging session, compared to how it works in ISO 15118-2.

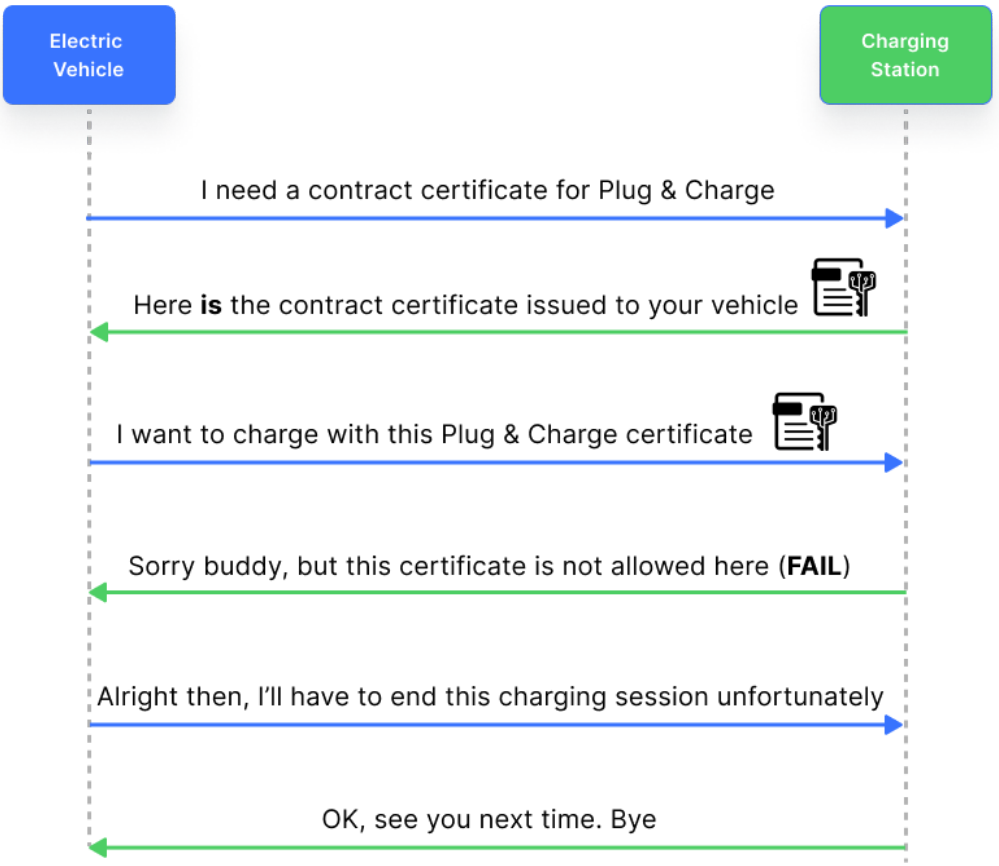

Fig. 6: ISO 15118-2 Contract Certificate handling

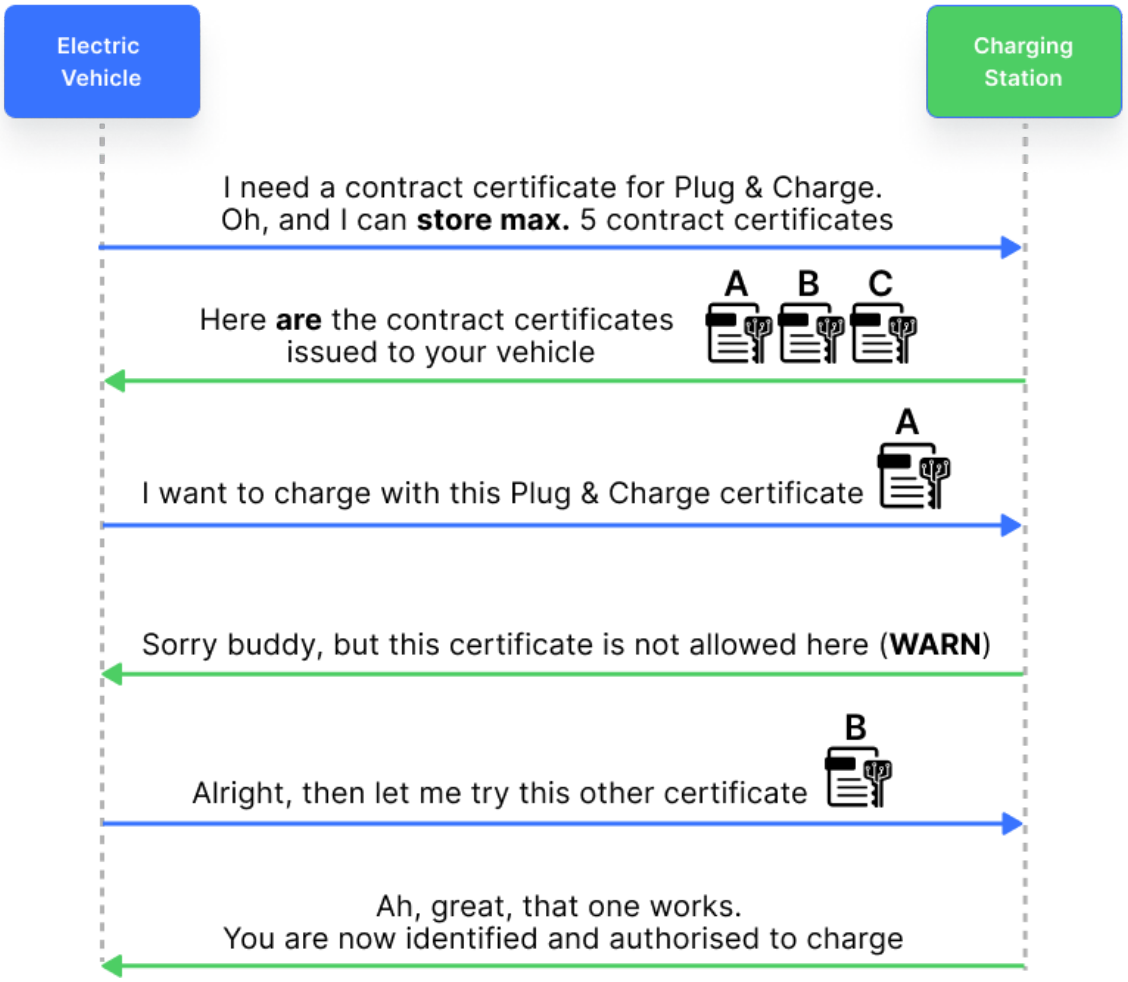

Fig. 7: ISO 15118-20 Contract Certificate handling

Step 3: Present the Contract Certificate to the charger and verify its authenticity

The actual identification via Plug & Charge includes several sub-steps. This involves validating the whole certificate chain, doing a replay attack check, and verifying that the presented Contract Certificate is indeed linked to an active and valid billing account. So let's dive into these sub-steps one by one, shall we?

Validate the certificate chain (offline/online)

The EV uses the Payment Details Request message in ISO 15118-2 (or the Authorization Request message in ISO 15118-20) to send the Contract Certificate together with the MO Sub CA Certificate(s)[11] to the charging station. The charging station, or its associated CPO backend, now need to:

[11] In this white paper, I refer to the market role that offers an electricity contract for your EV and issues the associated Contract Certificate as the Mobility Service Provider (MSP). This is the standard term used by most industry peers. However, in ISO 15118, this market role is referred to as the Mobility Operator (MO), and the associated certificates are issued by the MO Sub CA and MO Root CA.

1. Check that no certificate has expired. Each certificate has a validity period defined by the ‘notBefore’ and ‘notAfter’ fields, as shown in the example of a Contract Certificate when I introduced the concept of digital certificates.

2. Verify all digital signatures, from the Contract Certificate to the corresponding root CA certificate, which could be either the V2G Root CA Certificate or a dedicated MO Root CA Certificate, if the MSP decided to operate a root CA of its own.

The charging station can check the expiration of each certificate offline, it doesn’t need a cloud-based CSMS for that. Checking the digital signatures all the way to the root certificate only works offline if the charging station has the right root certificate installed that matches this Contract Certificate chain, and if the charger is configured to do this check offline (can be configured via OCPP 2.0.1).

If the CPO stores the corresponding MSP root certificates in the cloud, the charger needs to send the Contract Certificate chain via OCPP 2.0.1 to the backend and let the CSMS[12] handle it.

Check the revocation status (online)

This step requires a charging station to be online as we need access to the OCSP responder to retrieve the revocation status of the CPO Sub CA Certificate (both ISO 15118-2 and -20) and the Contract Certificate (ISO 15118-20 only). You can read the URL of the OCSP responder from the certificate’s ‘AuthorityInformationAccess’ field. The CA who issued a certificate usually also operates an OCSP responder.

Check that a valid billing account exists (online)

The CPO wants to get paid for the energy they deliver to an EV. This financial transaction is governed by a B2B contract between the CPO and the MSP who issued the Contract Certificate. Naturally, the CPO wants to make sure that the billing account (the legal contract associated with that Contract Certificate) is still valid and has not been suspended or cancelled. The EV driver might not have paid their monthly fees and the MSP decided to suspend the contract – you never know in advance.

Therefore, it’s crucial for the CPO to verify the contract’s validity with the MSP and obtain an acknowledgement from the MSP. This ensures that the CPO will get paid for the energy delivered.

How does the CPO know which MSP to contact? This information is stored in the EMAID, the E-Mobility Account ID, which is the identifier for the billing account. See Step 3 of the Contract Certificate provisioning process to refresh your memory on the EMAID structure if needed. The EMAID’s provider ID uniquely identifies the MSP, and the CPO would probably have a mapping table in place between the provider ID and a

[12] I use the terms ‘backend’ and ‘CSMS’ (Charging Station Management System) interchangeably.

web service URL of that MSP to check the validity of a Contract Certificate. Or, if the CPO uses a roaming platform like Hubject, they can use a dedicated web service without needing a mapping table.

Avoid a replay attack (offline)

“What’s a replay attack?” might be your first question.

A replay attack is like a digital impersonation. Imagine sending a message to a friend, but someone sneaky observes how you send it and copies your actions. Later, when you're not around, they pretend to be you and resend the same message to your friend. Your friend, assuming it's you again, may act on the message without realising it's a fake.

In the digital world, a replay attack works similarly. Hackers intercept and capture data transmitted between two devices (like the EV and the charger). Then, they replay the data, pretending to be the original sender, deceiving the recipient into thinking it's a legitimate communication. This can lead to unauthorised access, fraudulent transactions, or other harmful consequences. To prevent replay attacks, security measures like timestamps, unique identifiers, and secure protocols are used to ensure that the data being exchanged is fresh and hasn't been tampered with.

Protection against replay attacks is also baked into ISO 15118. When the charging station responds to the EV with a Payment Details Response, it sends a random 128-bit value called ‘GenChallenge’ (for ‘generated challenge’). The EV then needs to copy this value into the following Authorization Request message and digitally sign this message with the private key that is associated with the Contract Certificate’s public key. The charging station, having received the Contract Certificate with the previous Payment Details Request message, can now validate the Authorization Request’s signature with the Contract Certificate’s public key – et voilá, the EV is finally authenticated and authorised for charging. The charger does not need to communicate with the backend to avoid replay attacks, which is why I marked this step as ‘offline’. Just ensure you have a secure random number generator to create the challenge.

Keep also in mind that the charger must not store the Contract Certificate chain it received from the EV beyond the lifetime of that charging session. As soon as the session terminates, the Contract Certificate must be deleted from the charger.

That’s it. Next up, the EV and charger continue with the ISO 15118 communication sequence to exchange charging parameters and the charging schedules to finally start the energy transfer.

Can we do Plug & Charge with an offline charger?

That's a good, but tricky question to answer. The short answer is 'no'. The longer answer is 'it depends'.

What happens if the charger is temporarily offline due to a bad cellular connection? If you can't verify that the billing account related to the Contract Certificate is still active, you as the CPO run into the risk of losing money: if later on, when the charger comes back online, you find out that the account has actually been suspended. The MSP won't reimburse you for the energy you've delivered to the EV.

Obviously, we want the EV driver to be happy and charge their cars as a general rule. They shouldn't have to worry about the particularities of Plug & Charge. They just want it to work.

Here's what I would suggest: If the charger is temporarily offline, but you want to enable Plug & Charge for a particular charging session, configure your charger to authorise while offline. If later on the MSP tells you "sorry buddy, but I have no active billing account for this EMAID", then you put this Contract Certificate and/or EMAID on your 'block list' and the next time that same EV with that same Contract Certificate tries to do Plug & Charge, you only allow it if the charger is online. If the charger is offline, you only allow EIM. And if Plug & Charge is successful, you can remove this EMAID from the block list.

I'm happy to hear your thoughts on this approach.

Current ecosystem providers

For several years, there has only been one V2G PKI provider, namely Hubject. But as the e-mobility market matures, other players have voiced their interest in this role and the question of neutrality and market monopoly has sparked a discussion on how this ecosystem should evolve.

In this chapter, you'll get an overview of the current status quo and where the industry is headed.

Hubject

Since 2019, Hubject has been operating a V2G PKI ecosystem for Plug & Charge, including the V2G Root CA, the Certificate Provisioning Service (CPS) and the various data pools (Provisioning Certificate Pool, Root Certificate Pool, Contract Certificate Pool), which I mentioned in the chapter on provisioning a Contract Certificate to the EV. Their solution is based on ISO 15118-2, ISO 15118-20 and the application rule VDE-AR-E 2802-100-1[13]. An ever-increasing number of partners have adopted the standard and implemented Plug & Charge using Hubject's V2G Root CA and ecosystem.

Hubject partners with Nexus Group, an information security company that is an established expert in operating PKIs, and passed the information security audit in compliance to ISO 27001:2013. This international standard outlines the requirements for establishing, implementing, maintaining, and continuously improving an information security management system within the context of an organisation. By passing this audit regularly, PKI operators can prove the quality and security of their processes to the EV charging industry.

Hubject has been operating their V2G Root PKI in Europe and North America since 2019. Early April this year, they announced offering a V2G PKI also in Asia. Autocrypt from South Korea will likely be among the first customers of this new service offering. You can download Hubject's certificate policy documents for each market on their website.

[13] I have been working on the first and updated version of this application rule with a group of experts from 2016 to 2018 and was the lead author of this document. This experience proved to be very helpful when helping CharIN to review their 'Interoperability Guide – Public Key Infrastructure (PKI) use cases', which they published on 30 April, 2023.

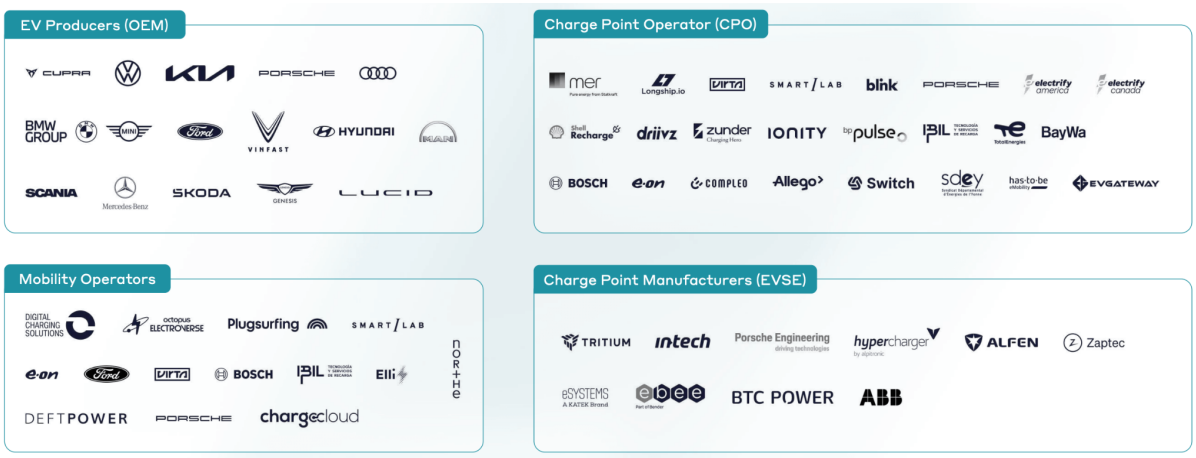

Fig. 8: Participants of the Hubject Plug & Charge ecosystem
(Source: Hubject's "State of the Industry Report 2023")

CharIN

CharIN announced its operational start of a V2G PKI in September 2022. Irdeto, an expert in digital platform cybersecurity with more than 50 years of experience, and UL Solutions, a safety, security, and sustainability company, will operate the V2G PKI on behalf of CharIN. Irdeto launched a new service called CrossCharge in April 2023, which they offer as a complete set of managed services that creates, distributes, discovers, validates and revokes OEM Provisioning Certificates and Contract Certificates.

You can find the terms and conditions, the root CA itself for the QA and production environment, the certificate policy documents and governance guidelines as well as a price list on CharIN's PKI page. They offer support for ISO 15118-2 and have plans to support ISO 15118-20 as well.

Time will tell how well their service will be received in the market and when vehicle manufacturers will adopt and install CharIN's V2G Root CA Certificate into their EVs.

More players are coming

French roaming platform provider Gireve is also known to have plans to operate its own V2G Root PKI and establish PKI services in collaboration with digital security company Thales. However, they have not yet published a specific release date.

The Society of Automotive Engineers (SAE) International, a professional association and standard development organisation based in the US, is also working on an SAE EV Charging PKI. As of yet, there is no public information available on the progress of their project or what their plans are regarding interoperability with the CharIN and Hubject PKI.

PKI interoperability and market governance

As multiple V2G PKI operators enter the market place, we need to make sure that they are interoperable. That means these PKIs need to be interconnected and operate under the same data security standards and market governance rules. Otherwise, that seamlessly working Plug & Charge ecosystem I've been talking about isn't really going to fly. We need a level playing field for MSPs, CPOs, utilities and EV manufacturers to avoid unfair competition and facilitate freedom of choice for end users.

PKI interoperability

In a market with multiple PKI operators, interoperability can be achieved either through Cross Certification or Cross Recognition using Certificate Trust Lists (CTL).

ElaadNL, a partnership of Dutch grid operators, published a knowledge piece called "Public Key Infrastructure for ISO 15118 – Freedom of choice for consumers & an open access market" in May 2022. In this publication, the authors offer an in-depth explanation of cross certification and cross recognition with CTLs. Let me provide you with a quick introduction into each concept.

Cross certification

In Step 1 of "How a Plug & Charge session works", we discussed how the EV establishes a secure communication link with a charging station. You may remember that the EV must be able to validate the SECC Certificate, which is issued under a particular V2G Root CA. If the EV does not hold the corresponding V2G Root CA Certificate, a secure channel cannot be established. However, the EV manufacturer cannot anticipate all the charging operators their EV drivers will visit, and even so, an EV may not be able to store all the necessary V2G Root CA Certificates. In this context, cross-certification between the certificate chains issued through the multiple V2G Root CAs can open the door for cross-V2G charging services.

For example, if a German V2G Root CA and a French V2G Root CA cross-certify each other, any EV that holds only the German V2G Root CA Certificate in its storage can charge at a charging station that has an SECC Certificate issued under the French V2G Root CA.

As good as this approach sounds, it does have two primary downsides to cross certification:

1. Reason number one is that ISO 15118-2 was not designed for cross certification. Thirteen years ago, when the ISO 15118-2 working group started out, the idea was to have a single V2G Root CA per continent and the need for cross certification wasn't really on the radar. This means that there isn't a way to implement cross certification between V2G Root CAs with ISO 15118-2 that guarantees interoperability. Only ISO 15118-20 was designed to allow cross

certification, which means that an additional Cross Certificate type is specified in the document and it allows a certificate chain to contain up to four certificates: one leaf, two Sub CA certificates and one Cross Certificate. Various ways of facilitating cross certification, like mutual and unilateral cross certification on both Root CA or Sub CA level, are described in Annex H.1.5 of ISO 15118-20.

2. The second aspect to keep in mind with cross certification is that cross certification may complicate the certificate policy management of the PKIs that cross sign each other. Consider for a moment what happens when organisation A cross certifies organisation B's certificates: The security level of B's PKI will be affected by A as PKI-B should fulfil the required security levels of PKI-A because the validator that trusts A will go through the certificates of PKI-B believing that these certificates are issued by PKI-A. If the certificate chain of PKI-B is compromised, and hence should not be trusted, the validator (e.g. EV) that trusts PKI-A can falsely trust the chain because the chain is apparently signed by the PKI-A. Therefore, before cross certification, A makes sure B's PKI policy is compatible with A's PKI. (I hope I didn't confuse you too much with this paragraph, but it's really not easy to explain this in simpler terms.)

Given that cross certification is not necessarily a straightforward solution in the realm of ISO 15118, the industry is currently leaning more towards Certificate Trust Lists.

Cross recognition with Certificate Trust Lists (CTL)

To ensure that certificates issued by different Certification Authorities are trusted, a CTL is used. It's like a master list that contains all trusted root certificates from various CAs that are considered valid within the V2G PKI ecosystem. By referring to the CTL, the vehicle and charging station can verify the authenticity and integrity of each other's certificates, enabling secure and interoperable communication for EV charging.

The maintenance of a CTL in the context of ISO 15118 V2G Root CA interoperability could be handled by an industry-approved governance body or consortium. This entity ensures that the CTL is regularly updated to include new trusted root certificates from recognised CAs. The maintenance process involves adding new certificates to the list when they meet specific security and compliance criteria and removing any certificates that are no longer considered secure or valid.

AFIR and SAE – Interop initiatives in the EU and North America

The Alternatives Fuels Infrastructure Regulation (AFIR) is a European regulation that defines, among other aspects, the requirements for interoperability among different EVs and charging stations. Specifically, the Sustainable Transport Forum's (STF) sub-group on "Governance and Standards for Communication Exchange in the Electromobility Ecosystem" is currently dealing with the market governance rules for

an interoperable ISO 15118 V2G PKI ecosystem, including the management of a Certificate Trust List. AFIR also paves the way for a user-friendly recharging experience, with full price transparency, common minimum payment options and coherent customer information across the EU.

The AFIR is about to be published in June 2023. My current understanding is that the European Commission will run a public tender to source an independent and trustworthy party in charge of managing a CTL for all V2G Root CAs. This can easily take two to six years, with some bets on four to five years. As we know, European institutions don't move at lightning speed and the decision will likely be made through a public tender. We'll see whether a rather neutral organisation like the EU's Joint Research Centre or a specialised organisation with deep expertise in cybersecurity will be chosen. Until then, the best way forward is for EV manufacturers to do their own assessment of existing V2G Root CAs and to install the trusted V2G Root CA Certificates into their vehicles.

AFIR is, of course, a European initiative and we'll see whether other parts of the world will be inspired by this regulation to adopt similar market rules in their regions. The US-based standardisation organisation SAE International, for example, is involved in the STF sub-group to exchange their views and time will tell how this will eventually pan out in North America.

As you can see, PKI interoperability is not an easy topic. It's not rocket science, technically it's feasible to achieve a solution in a rather short amount of time. But it's the agreement on interoperability and market governance rules and the fact that different stakeholders have different opinions that doesn't make this any easier. It's like Democracy: no-one said it's going to be easy. But it's the best and most fair way of building a consensus that all parties can (hopefully) agree upon. PKI interoperability demonstrations like the one between ElaadNL, Vedecom an Hubject, and workshops like the Joint CEC-ElaadNL Hybrid Workshop on PKI and Governance in June during EVS36 will help the industry find a common solution that scales globally.

CharIN is also working on an white paper called "Interoperability Guide – Public Key Infrastructure (PKI) use cases", which aims to define all relevant use cases for Plug & Charge, based on the application rule VDE-AR-E 2802-100-1. The first version was published April 30, 2023, and I'm currently working with other authors on an updated version that will reflect upon interoperability between different V2G Root CA providers and how to best support multi-contract handling in the vehicle.

Personal remarks on PKI interoperability

The only reason why we need a CTL is that some organisations or companies feel that a single, commercial V2G Root CA operator may not be the best idea. Why? Because the whole ecosystem would then potentially be exposed to a monopolistic situation where one company dictates prices for V2G Root CA certificates. That's why CharIN

started joining the ranks of a V2G Root CA operator, and then choosing Irdeto as a supplier for managing the IT ecosystem after running a tender.

But one thing should be clear to everyone: the more V2G Root CA operators, the more complex this whole ecosystem will become – and running a Root CA is not really a money-generating business. Yes, having more than one V2G Root CA operator fosters competition and can bring prices down, but there needs to be a balance to it. Searching for a governing body that manages a CTL feels a little bit like kicking the can down the road, or pushing the problem just one level higher. At least, if we can agree on a CTL manager that is approved by the European Commission, we may be able to leave the discussion about a 'sufficiently independent' provider of a V2G Root CA finally behind us.

Market governance rules

Interoperability on a technical level is similarly important as making sure that the whole ecosystem is based on fair and equal rules for all market participants to ensure a level playing field that fosters healthy collaboration and competition.

You can tell that fair market rules are a topic of high interest, not only because of the upcoming AFIR regulation but also due to the fact that several organisations have already published their standpoints. The most prominent examples are ElaadNL's Public Key Infrastructure for ISO 15118 - Freedom of choice for consumers & an open access market (2022), ChargeUp Europe's Public Key Infrastructure Market Principles and Hubject's State of the Industry Report 2023 (slide 11).

The core message of these statements can essentially be boiled down to these three principles: transparent governance, data protection and cybersecurity, and freedom of choice for the EV driver:

Transparent governance

Transparent governance ensures that all market players act on a level playing field. Information on the operational processes of any V2G Root CA must be publicly accessible. Market players should be able to easily download the Certificate Policy and other relevant documents from the operator's website. To establish trust in the ecosystem, a central, independent (non-profit) organisation should operate the Certificate Trust List.

Data protection and cybersecurity

To aid understanding, these documents should be supported by additional information regarding external, independent security audits to ensure that all V2G Root CA operators rely on a similar level of minimum requirements regarding data protection and cybersecurity. In particular, access to the ecosystem needs to be protected and

any sensitive information, such as competitor data (e.g. MSP contract information) or information about end consumers, need to be protected under GDPR.

Freedom of choice through non-discriminatory contract handling

To ensure non-discriminatory access for services such as Plug & Charge, all EVs should support the installation of Contract Certificates based on driver preference. Car manufacturers as well as MSPs should support multi-contract handling. The installation, update, removal and prioritisation of a Contract Certificate in the EV must be defined to give full control to the EV driver, for example through their in-car display or mobile app. This ensures a level playing field for car OEMs and MSPs, and it guarantees that an EV driver can charge at any publicly accessible charging station using any service provider. Therefore, car OEMs need to provide all relevant information, including the Provisioning Certificate Identifier (PCID), which identifies the EV, to the customer in a simple and straightforward way. Only then can an MSP issue and provision a Contract Certificate to this customer's EV.

The Open Plug & Charge Protocol

To encourage the development of an interoperable, non-proprietary communication protocol for all emerging ISO 15118-2 and ISO 15118-20 solutions, Hubject has initiated a governance group alongside other industry stakeholders in September 2022. To kickstart the project, Hubject has offered its Open Plug&Charge Protocol as a technical foundation that can evolve based on the input from all stakeholders participating in this governance group. OPCP is based on the application rule VDE-AR-E 2802-100-1, which defines the inter-communication and processes between all market players for provisioning a Contract Certificate. The protocol is already being used by many market participants, including most of the major EV manufactures (see Hubject's ecosystem overview).

For the sake of (more) neutrality, CharIN is now managing the protocol governance group. After lengthy discussions, a Charter has been adopted to establish the governance framework for the communication protocol, and a steering committee is about to be put in place. The name of the protocol may change but a decision has not yet been made. The group's primary goals are:

- Develop and establish a commonly accepted protocol, taking into account existing and freely available protocols
- Provide backwards compatibility to Plug & Charge ecosystem solutions already implemented in the market
- Add new use cases and functionalities that are not yet part of OPCP
- Deliver a first version of the protocol quickly – within the year 2023

Software interoperability and conformance tests

ISO 15118 and the surrounding PKI technology is complex. Ensuring interoperability between different market vendors is paramount to make EV drivers trust and accept this technology. This will have a significant impact on the pace in which we can electrify mobility and help decarbonise transportation.

As of writing this white paper, we still lack a certification program for ISO 15118 and Plug & Charge that is based on ISO 15118-2 and -3 and the associated conformance tests defined in ISO 15118-4 and -5. Currently, we only have a certification in place for what is called CCS Basic, which essentially means basic AC charging using the PWM signalling mechanism described in IEC 61851 and ISO 15118-3 and DC charging based on DIN SPEC 70121.

DIN SPEC 70121 is a predecessor to, or early subset of ISO 15118, which focuses solely on DC charging. This German specification was first published in 2012 to kickstart the DC charging market as the publication of ISO 15118 was still two years away. DIN SPEC 70121 was revised in 2014, the same year ISO 15118-2 was published as an international standard. The plan was to replace DIN SPEC 70121 in the market with ISO 15118-2, but as it turns out, nothing is as permanent as a temporary solution. Many EVs and charging stations with DIN SPEC 70121 support have been deployed in the market over the past decade and we'll end up having to support this legacy technology for a few more years. DIN SPEC 70121 does not support cybersecurity and, subsequently, also not Plug & Charge.

For ISO 15118-2 with Plug & Charge (CCS Advanced) and ISO 15118-20 (CCS Extended), there is no certification available yet. However, a certification process for CCS Advanced is underway and the current estimate is that we'll be able to certify EVs and charging stations for Plug & Charge by the end of 2023.

Ideally, only those EVs and charging stations that have been certified for Plug & Charge should be allowed to carry the official Plug & Charge logo, which was first unveiled at the CharIN Testival Europe in Poland in summer 2022. I am concerned that manufacturers of EVs and charging stations are capitalising on this logo without proper certification, which may be a disservice to the end customer. Imagine the frustration and mistrust if an EV driver is trying to charge their EV at a charging station carrying the logo – but the charging session fails due to interoperability issues.

Fig. 9: The official Plug & Charge logo introduced by CharIN

In the following section, you'll learn more about the available test laboratories, interoperability test events and test system providers.

Test laboratories

Officially recognised test laboratories for the CharIN Conformance Test System (CCTS) are DEKRA Certification B.V. and the Korea Electrotechnology Research Institute (KERI).

CharIN Testivals

The lack of a proper ISO 15118 and Plug & Charge certification program is one of the main reasons why these hands-on testing events exist. They bring together representatives from the car manufacturer and charger manufacturer industries to test their products for interoperability.

The first testing event took place in 2014 at the Technical University of Dortmund. Eventually, Verisco, a spin-off of the TU Dortmund, founded by Jens Schmutzler and Sven Groening, took care of organising these events on a regular basis each year. From 2019 onwards, CharIN took over as the official organiser of these so-called "Testivals". They are still supported by Jens and Sven, who by now have sold their company to Keysight Technologies and continue their great work with the help and resources of a bigger organisation.

These CharIN Testivals take place in North America, Europe and Asia several times a year. You can find the latest information about upcoming events as well as great video impressions of past Testivals on their website.

These CharIN Testivals serve as important events to test the latest prototypes for compatibility with other market vendors. Additionally, they offer great opportunities to network with industry peers and find out about the latest tech developments in our industry. These Testivals also allow so-called 'Observers' without test equipment to participate.

Conformance test system providers

Conformance test system providers offer test tools, test suites, and testing frameworks that allow manufacturers and developers to verify their products against defined standards. These tools may include software applications, hardware devices, or a combination of both. They enable users to perform various so-called happy-flow and non-happy flow tests to determine if their products meet the required standards, specifications, or interoperability requirements.

Within the ISO 15118 standards series, ISO 15118-2 is the main part of ISO 15118 that defines all the messages and message sequences the EV and charger need to exchange during a charging session. This Part 2 covers everything from the network layer (TCP/IP, TLS, etc.) to the application layer (the actual messages and data types). ISO 15118-3, on the other hand, covers the lower level communication, i.e. how the EV and charger set up a data link using power line communication.

The conformance test cases that cover all "happy" and "non-happy" flow tests for ISO 15118-2 are defined in ISO 15118-4. Likewise, the conformance tests for ISO 15118-3 are covered in ISO 15118-5. Below is a picture that summarises the relationship between the various ISO 15118 documents.

You only need to take a look at the conformance test documents if your business is selling conformance test systems that implement these test cases. Here's a list of currently available conformance test system providers, with links to their websites. I highly recommend purchasing test equipment from one of these providers as this will increase the quality of your product and the likelihood of being interoperable with other solutions on the market – which in the end leads to happier EV drivers.

- Keysight (see also announcement that the DEKRA test lab uses Keysight)
- Vector Informatik (EV and EVSE)
- Comemso
- dSPACE

ISO 15118 User Group

The ISO 15118 User Group is an online forum where early adopters and developers can discuss any issues, inconsistencies or ambiguities they come across while implementing and testing ISO 15118. It first started in 2013 when the industry began implementing ISO 15118-2. This user group was revived last year to provide a place to

quickly discuss solutions for any issues while implementing the new ISO 15118-20 standard.

You can request to join the ISO 15118 User Group using this link. The ISO/IEC Joint Working Group (JWG) is moderating this forum and holding regular online meetings to go over the latest list of issues and to discuss ways to resolve them. The issues that were discussed in the early days of implementing ISO 15118-2 were all directly influencing the development of ISO 15118-20, and the second edition of ISO 15118-2. Similarly, currently ongoing discussion will influence the next edition of ISO 15118-20. Unfortunately, it will take at least two years, if not more, to publish a second edition of ISO 15118-20.

Luckily, we found a way to fast-track some more urgent issues we came across already: The JWG decided to work on an so-called ‘amendment’ of ISO 15118-20, which we plan to publish by the end of 2023. The amendment will include some of the most upvoted issues in the user group as well as a proposal for a better support for AC V2G and grid codes. Switch is currently leading the task force to work out the AC V2G proposal.

The business case for market participants

In this chapter, we'll delve into the business case for implementing Plug & Charge technology across the various market roles of commercial EV charging. From charger manufacturers (charger OEMs) to Mobility Service Providers (MSPs), car manufacturers (car OEMs), and Charge Point Operators (CPOs), we'll explore how Plug & Charge can transform the user experience and enhance the business case of EV charging.

Plug & Charge is a seamless process for both AC and DC charging that brings a hassle-free and hands-off experience for EV drivers of all kinds. One of the undeniable benefits of Plug & Charge is the ability to automate secure charging and billing without any driver involvement. With zero driver activity required, payment is authenticated and automated through pure machine-to-machine communication. Now this might seem basic: One less step in a user journey. One less element of human interaction, one less click that can be faulty and break. But it really is: A huge plus.

One less click: how Uber disrupted the transportation industry

Uber, a game-changer in the transportation industry, exemplifies the transformative power of streamlining UX and simplifying user journeys: With a single press of a button, the entire journey is set in motion. When you arrive at your destination, the driver thanks you, and your credit card is automatically charged at the set price for the trip – no extra click necessary. This cashless and transparent approach to pricing and user experience set Uber apart and was a gateway to disrupting the industry with a fundamentally different and new approach.

Similar to Plug & Charge technology, Uber eliminates the user involvement in payment, and as such the need for cash or outdated credit card machines. The simplification of the payment process on improved customer experience was key to Uber's success and the pivotal turning point for an entire industry as Uber started to conquer and disrupt not just taxi rides, but the entire transport sector.

The driving force behind Plug & Charge lies in its ability to do just that: disrupt the charging process with machine-to machine communication while offering an unmatched quality lift for the wider user experience. This technology-driven shift impacts the entire EV charging industry. From charger OEMs to MSPs, car OEMs, and CPOs, all benefit from the enhanced security and convenience of the Plug & Charge process.

Charger manufacturers

Plug & Charge helps charger OEMs gain a competitive edge and increase their market share in the EV charging industry. Here's why:

1. Enhanced eligibility for tenders and funding: ISO 15118-powered Plug & Charge compliance allows charger manufacturers to meet the requirements of public funding, particularly in the US. Being eligible for funding schemes such as the NEVI funding makes their products more attractive for Charge Point Operators seeking to expand their networks. This opens up opportunities to win more contracts on a better price tag for the network operators and provides a significant advantage over competitors.

2. Strong cybersecurity: Implementing Plug & Charge technology demonstrates charger OEMs' commitment to innovation and data security. Robust cybersecurity measures protect data and prevent fraud, establishing trust and confidence among customers. It also allows to scale network size and leverage additional customer facing services with peace of mind.

3. The best charging experience: User experience (UX) and hardware design are crucial for charger OEMs. It's how customers perceive and interact with their products, rendering a pleasant – or not so pleasant – overall experience. Providing such an integral interface element in the user journey of EV charging means it is key for charger OEMs to distinguish themselves from the competition, not just with outstanding physical product design, but with an exceptional digital surface as well. And chargers are becoming defining architectural elements of daily life – almost a lifestyle product as such. As a result, the UX – encompassing haptics and surface design – is vital for increasing demand for their products.

Mobility Service Providers

For MSPs, integrating Plug & Charge technology presents significant benefits. Here's why they should consider adopting Plug & Charge:

1. Winning more customers: Plug & Charge simplifies the charging process. The driver can start a charging session simply by plugging in the vehicle. No card or app needed. This means that authentication and authorisation of charging, payment and billing are all automatically approved from the car's central dashboard, eliminating the need for user interaction at the charger via third party media such as cards or smartphone apps.

2. Trailblazers of innovation with strong cybersecurity: Implementing Plug & Charge positions MSPs as forward-thinking providers in the mobility sector. The robust cybersecurity measures associated with Plug & Charge offer peace of mind to customers, assuring them that their data is protected, and transactions are secure.

3. Differentiation through customer obsession: Offering the final interface to the end customer and driver designates the MSP business to offer a superior customer experience, building on the streamlined simplicity of Plug & Charge.

Integrating the process into the wider business area of in-car search and navigation, as well as other services looking to increase the convenience of the overall experience will attract and retain customers who value convenience and efficiency to up their life. This can be achieved by providing additional services, such as dedicated electric forecourt operations for serviced charging and catering or dedicated customer care on the site. See these latest examples from Gridserve or eccovia. Such an enhanced value proposition allows MSPs – as well as CPOs incorporating this role into their offering – to differentiate themselves from competitors, encouraging customers to choose MSPs that provide a comprehensive and easily accessible charging infrastructure over less secure and forward looking charging methods.

Car manufacturers

Car Manufacturers can unlock numerous advantages by embracing Plug & Charge technology in their EVs. Here's why they should consider integrating Plug & Charge:

1. Winning more customers through a premium user experience: Plug & Charge simplifies the charging process, allowing EV drivers to connect and charge effortlessly. Car OEMs prioritising the best charging experience can attract and retain a larger customer base, enhancing their market share and brand reputation.

2. Comfort driver and co-drivers with strong cybersecurity and forward-looking innovation: Implementing Plug & Charge technology demonstrates car OEMs' commitment to technological innovation and customer satisfaction. Robust cybersecurity protects sensitive data and prevents fraudulent activities, providing peace of mind to both car owners and the OEM. And with the current ISO 15118-2 powered version acting as pre-runner to the coming ISO 15118-20 powered Plug & Charge, a whole new array of services will be accessible with a simple over-the-air upgrade.

3. Streamlining multi-contract handling: Teach your vehicles to perform reliably across technical borders and geographical locations. With the detailed information provided in this white paper (here and here) you can steer and lead the implementation of Plug & Charge across several PKIs and regions. This not only allows alignment with local legislative restrictions and frameworks and ensures a frictionless roll-out across global production lines. But it also makes sure your customers can choose deliberately which service provider to choose for a charging session. Looking ahead, this opens opportunities to expand the business area of your hardware-centric market role to a service-oriented offering in the wider energy market. It also unlocks dedicated offerings that support use cases such as the charging, billing and cross-settlement of corporate fleet charging in private settings or supply of energy supplied from sustainable sources only.

Charge Point Operators

For a CPO, Plug & Charge holds the potential to not just future-proof your investment but also tap into additional target audiences and revenue streams:

1. Integration with existing infrastructure: By integrating Plug & Charge into their existing charging infrastructure, CPOs can leverage their current investments and infrastructure while adopting the benefits of this technology. This works with charging stations that are equipped with a HomePlug Green PHY modem for power line communication, like CCS-based chargers. AC charging stations with HomePlug GreenPHY modems are only starting to come to market.

2. Access a solvent target audience rolling on premium vehicles: Plug & Charge brings an audience that is willing to pay for convenience and superior service. This 2022 study of EVBox finds EV drivers are often highly educated and full-time employed. Adding the latest findings of Hubject, we learn that the number of EVs equipped with Plug & Charge on the road quadrupled throughout 2022, hitting a milestone of 100% growth from the third to fourth quarter. Bottomline: Adding this segment will improve your forecast, your financial rating and the overall profitability of your charging network.

3. Future-proof infrastructure: Embracing Plug & Charge allows CPOs to build a forward-looking charging infrastructure. By adopting this technology, CPOs align their charging sites with the latest industry standards and customer expectations, excel in convenience and thus become a first-choice among a growing base of customers. This will ultimately yield EV drivers happy to return to a site on a regular basis

Overall, adopting Plug & Charge technology offers substantial benefits for all market players. By embracing this innovative solution, industry players can enhance their competitive advantage, attract more customers, increase customer retention due to unmatched convenience and establish their businesses as organisations that take innovation and data security seriously. Moreover, Plug & Charge technology is built on the robust ISO 15118 standard, ensuring interoperability, cybersecurity and a forward-looking future readiness that can be unlocked by a simple over-the-air update. As the industry evolves, the upcoming ISO 15118-20 edition promises the even greater potential for businesses, such as bi-directional charging to enable V2H and V2G use cases. By aligning with this standard, industry players can future-proof their offerings, and take advantage of emerging opportunities to lift their business evaluation.

The costs of implementing Plug & Charge

How much does it cost each of the market roles to implement Plug & Charge into their products and services. And how much more expensive will the charging experience become for the end consumer, the EV driver?

It's impossible to put an exact number to it as the implementation costs vary greatly from company to company. Do they implement the technology themselves or rely on third parties (make vs buy)? Which V2G PKI ecosystem will they use? And will they swallow the implementation costs or pass on parts of their costs to the EV driver?

The only pricing information I can provide is the pricing of the Switch products for CPOs (Switch platform) and charger OEMs (Josev), as well as the V2G PKI costs communicated by Hubject and CharIN.

Hubject V2G PKI

These are the costs for using Hubject's V2G Root CA and Sub CA services:

- **V2G Root**
  - No costs – available for free on the website
- **Issuing of Sub CA Certificates** e.g. CPO Sub 2
  - On demand
- T**est certificates from QA**
  - No costs, see open.plugncharge.hubject.com

And these are the costs for Hubject's Plug & Charge Ecosystem services**:**

- **Included**
  - Use of pools (RCP, PCP, CPS, etc.)
  - Certificate issuing if needed/necessary for the use case
- **CPO**
  - One-time 3,800 € onboarding
  - Per SECCID per year 0.99€ (negotiable on high volume)
- **MO**
  - One-time 5,000 € onboarding
  - Option 1:
    - Generation of complete ContractPackages (using the V2G PKI Service)
  - Option 2:
    - Signing of Contract Packages (Using MO independent PKI)

    - Price per EMAID (ContractID) → starting with 0.04€ per year

- **Car OEM**
    - OEM individual pricing – based on the needs of the customer
    - Usually onboarding project phase
    - Audit of car OEM PKI
    - Yearly fee for use of the ecosystem incl. PCP, CCP, Notification service etc.

CharIN V2G PKI

CharIN provides pricing information in a downloadable PDF on their website.

The Pros and Cons of Autocharge

When it comes to EV charging, security matters. EV chargers are not immune to attacks, especially as today's chargers currently use outdated protocols such as OCPP 1.6 and old technology like the DIN SPEC 70121-based Autocharge.

With the global push to electric mobility, this ecosystem becomes an increasingly interesting target for hackers. They are already aiming their attacks at electrical system vulnerabilities. And this is now being used in modern warfare. The US has alleged that Russia and domestic terrorists are attacking electrical grid systems as there is no real security at all, leaving the infrastructure vulnerable.

An attack has the potential to have a domino effect that puts the entire country in total blackout with no access to light, heat, refrigeration, phones and the Internet. In charging stations, these weak spots are located inside the stations and in the equipment controlling the connections between the EV and the grid.

The point I'm trying to make here is that the ISO 15118-based Plug & Charge and Autocharge are two completely different technologies with diametrically different security concepts. The terms 'Plug & Charge' (coined by ISO 15118, but, unfortunately, not trademarked) and 'Autocharge' are sometimes even used interchangeably. This is a disservice to EV drivers and the whole EV charging industry. It's important to reflect upon the distinct differences between these two technologies so that you can make an informed decision as to whether you should consider Autocharge or not.

Spoiler alert: DON'T use it in public charging environments where you bill your EV drivers.

How Autocharge works

Autocharge is the process that enables a charging station to authorise a CCS-equipped EV for charging. It is based on the unique identifier that the EV sends to a charging station when plugged in. Currently most EVs use the Media Access Control (MAC) address assigned to their communication controller. The MAC address is used as a network address for many network technologies including Ethernet, Wi-Fi, and Bluetooth.

Both the EV and the charger need to be equipped with a Homeplug Green PHY modem to enable power line communication, which allows the EV to send its MAC address. Power line communication is the basis for the DC only communication protocol DIN SPEC 70121 and, of course, ISO 15118 (which can be used for both AC and DC charging). Here's what happens in the background when using Autocharge:

1. You connect your EV to the charging station by plugging in the cable, which triggers the EV to send its MAC address to the charging station.

2. Autocharge relies on the Open Charge Point Protocol (OCPP) as a communication protocol between the charging station and its CSMS. The charging station uses OCPP's 'Authorize' request to send the MAC address it received from the EV to the CSMS.

3. The CSMS will then check if the received MAC address matches an entry in a whitelist of EV MAC addresses. In case of a match, the CSMS then sends an 'Authorize' response message back to the charging station. This confirms that your EV is allowed to charge and charging begins.

4. In case there is no matching whitelist entry, the CSMS will store the MAC address on the whitelist and send an 'Authorize' response to the charging station that denies the authorisation. As a result, the charging station may indicate that you need to authorise your EV using one of the other available methods like RFID card or smartphone app. Once you register for Autocharge with the operator's app, you'll then be able to use Autocharge for future charging sessions.

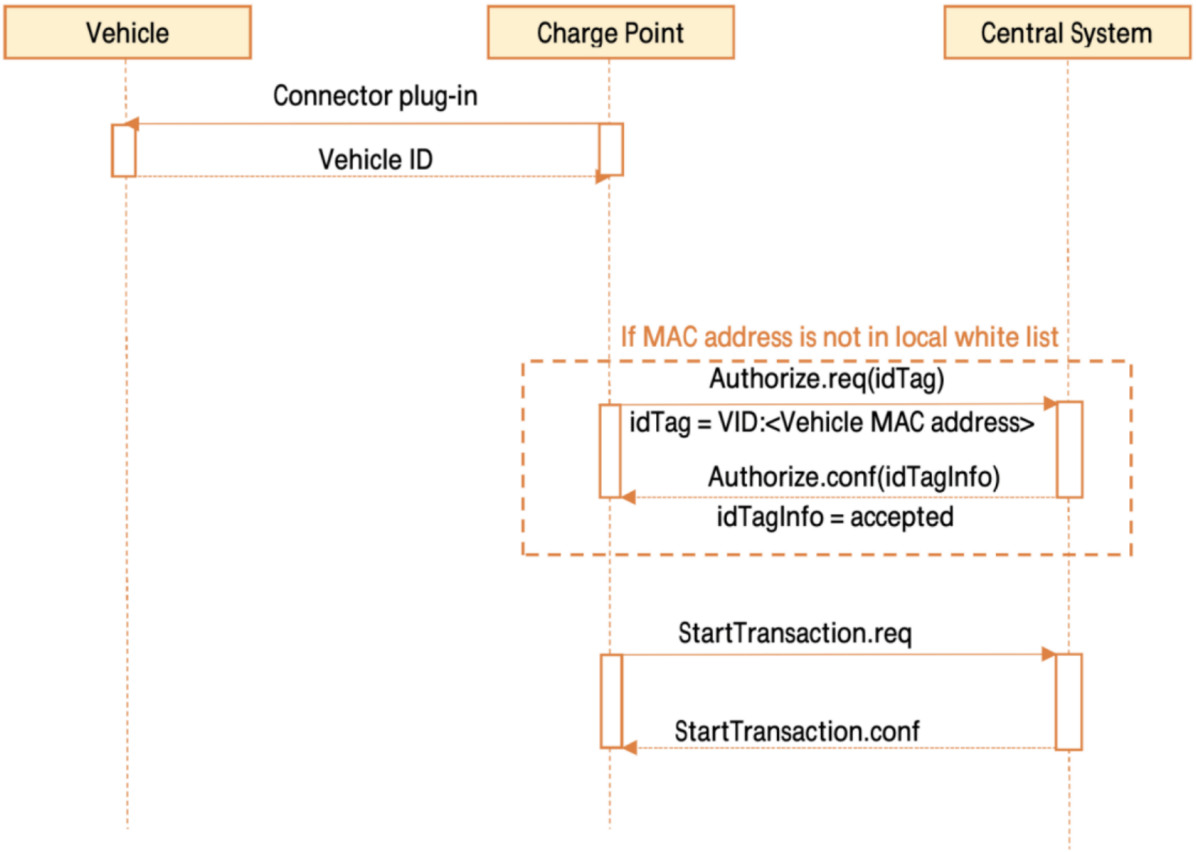

Fig. 10: How Autocharge works with OCPP (© Open Fastcharging Alliance, 2019)

The MSP usually links your EV's MAC address with your user account through a mobile app by first activating your EV for Autocharge and selecting the make and model, as explained on the German tech news portal heise.de or the websites of Dutch-based Fastned, Germany-based EnBW and US-based EVgo. Many, if not most, CPOs already maintain a whitelist of valid RFID tokens which they exchange with their roaming partners on a regular basis. For this, they use roaming protocols like OCPI or OICP. The same procedure applies to maintaining a whitelist of MAC addresses.

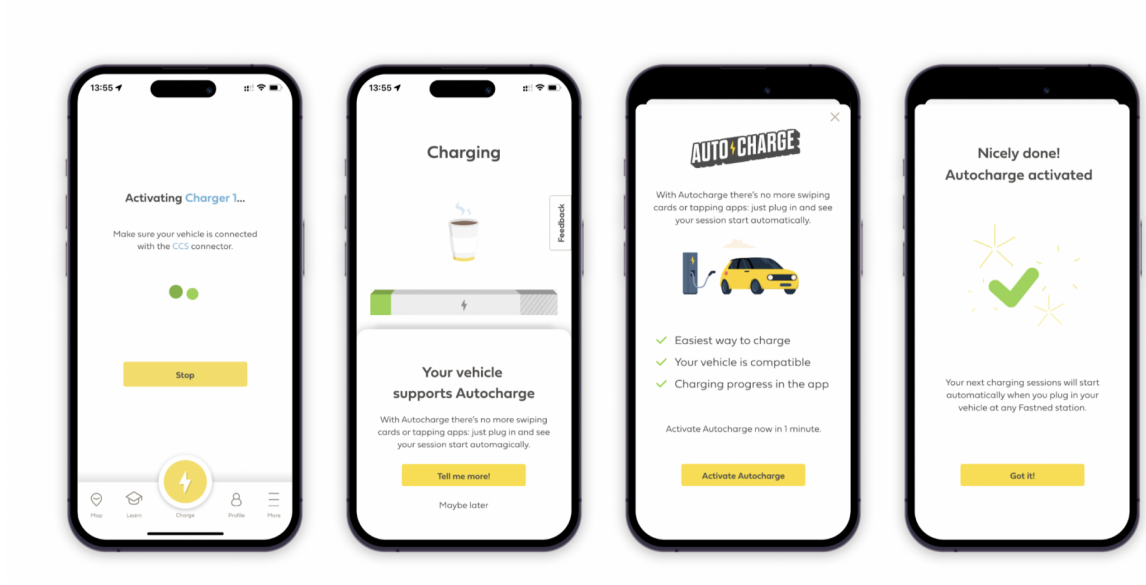

Fig. 11: Activating Autocharge on the Fastned app (Source: Fastned)

Key benefits of Autocharge

At first sight, there are some good arguments to use Autocharge over existing identification methods like RFID cards:

- Higher degree of user-friendliness over traditional authorisation methods like RFID cards and smartphone apps
- Higher level of data security compared to the widespread RFID technology (MIFARE Classic), as MAC addresses are not as easy to replicate as RFID cards
- Relatively simple implementation and, therefore, fast roll-out
- No major changes needed in backend IT systems, as Autocharge works with OCPP 1.5 and higher
- Functions with all existing and future CCS vehicles on the market that use unique MAC addresses (and before you ask: no, Autocharge does not work with CHAdeMO)

However, not everything that shines is gold and there are some significant security risks to take into consideration.

Why Autocharge is not a good idea

The utilisation of a MAC address or Vehicle Identification Number (VIN) to authorise a charging and billing process is problematic. Whenever a car connects to a station that uses Autocharge, its identifier is stored on a whitelist on the charger. This leaves valuable data stored on physical machines across entire continents, creating a data security and privacy nightmare. This is also why it is not supported by one of the world's largest car manufacturers, the Volkswagen Group. VW uses so-called rolling MAC addresses, which means that the MAC address changes every time the EV connects to the charger, rendering Autocharge useless. I've even heard that some car manufacturers use the same MAC address across all their vehicles, which again reduces the list of compatible EVs as Autocharge relies on 100% unique MAC addresses.

One might argue that MAC addresses are not considered to be 'personal data' as it is not tied to a person. However, the European Commission states that under Section 3. POINTS OF GRAVE CONCERN, page 11, paragraph 2, article 29 "it should be noted that these MAC addresses are personal data, even after security measures such as hashing have been undertaken."

The same goes for the VIN that is also being used in the latest version of Autocharge (Autocharge+). It is a number unique to each car, not unlike a Social Security Numbers is to people. With just a VIN, hackers are able to recover your name, address, nationality, age, etc. The reason why is the uniquely assigned hardware address of the network interface for devices like mobiles, cameras, computers, EV chargers, cars, etc. Thus, the user can be tracked regardless of location.

Another issue that MAC addresses pose is that they are not protected against spoofing, making Autocharge an insecure method. Potential man-in-the-middle attacks include manipulating the MAC address from the EV to the charger, from the charger to the charging station management system (CSMS) or from the CSMS to the Mobility Service Provider.

The result? Someone else can charge for free on your behalf, using your account. Now, you may argue that the risk of MAC spoofing is not that high and the associated financial risk may not be that significant. But with Autocharge being deployed mainly (if not only) at DC fast charging stations, the charged energy amount and resulting electricity cost may not be that insignificant anymore. And yes, I've heard the argument that using push notifications on your network operator's or MSP's app when someone tries to use Autocharge with your EV's MAC address can be used as a means of two-factor authentication. This can limit the risk – but then again: Isn't Autocharge supposed to provide that same worry-free, zero-touch charging experience?

One of the most common mistakes with Autocharge occur when renting a car: It sometimes happens that someone who rented a car forgets to deactivate Autocharge in the app after returning the car, only realising this when the next renter plugs it in. If the process is not noticed immediately and amounts are incurred, these users then occasionally contact the billing department for a cancellation and refund.

Where Autocharge may be useful

The best setting for Autocharge is in the fleet sector. When a fleet depot operator wants to create an efficient process for recharging their electrified delivery vehicles, a seamless plug-and-play solution is key. Fleet depots usually have some kind of access restriction, which lowers the risk of unauthorised third parties accessing the premises and trying to manipulate the identification tokens (MAC addresses).

If the fleet operator chooses compatible ones that do support unique MAC addresses, Autocharge might make sense. The lower implementation cost of Autocharge versus the potentially more expensive overhead of a Plug & Charge solution may justify the cybersecurity tradeoff.

On the other hand, one might want to consider the Private Environment (PE) scenario outlined in ISO 15118 and, in more detail, the aforementioned VDE application rule VDE-AR-E 2802-100-1. In a private environment, digital certificates are also used, but the underlying PKI is simpler. If you're interested in learning more about the PE scenario, feel free to reach out to me or sign up for the Advanced training on ISO 15118.

Switch platform and Josev – Plug & Charge ready solutions

At Switch, we do things a bit differently. From the very beginning, it has been clear that everything we do must be in line with four key principles to bring the maximum benefit for our customers:

1. Maximise return on investment
2. Provide ease of use
3. Enable a seamless, vertically integrated solution
4. Guarantee a future-proofed solution

The CSMS solutions currently on the market often focus on the monetisation aspect, with newer ones also starting to recognise the importance of intuitive design. However, none of them offer a vertically integrated solution to provide a frictionless charging experience, and most of them lack a future-proof solution.

Let me guide you through these four principles and how Switch addresses them with our products for both charger OEMs and CPOs.

Maximise return on investment

Switch can help position you in a saturated and competitive market place. By creating a value proposition that is superior to other EV charging networks, we help make EV charging a commercially viable business and maximise your return on investment. This is why Switch has procured specific features which are focused on reducing diagnostic overhead, maximising network uptime and improving value generation.

One part of this is to address the issue of cost. Switch recognises that investment in EV charging infrastructure can be costly, particularly for network operators who need to provide local infrastructure for their residents or customers (i.e. workplaces, landlords etc.) and for whom EV charging isn't currently a core part of their business strategy. We refer to these as the 'accidental' operators. By leveraging only the latest technology, Switch helps operators reduce their charging station network costs. In particular, maximising station uptime and reducing diagnostic costs are core components of our product proposition. Reliability, charger uptime and the ability to predict failures and disruptions (all cost-optimised) are important features of the Switch platform's OCPP 2.0.1 credentials. To learn more about the benefits of OCPP 2.0.1 over 1.6, head over to our online white paper section to download "Time's up. Say goodbye to OCPP 1.6".

For example, Switch has procured the Advanced Diagnostics feature by leveraging the potential of the OCPP 2.0.1 protocol and merging it with intuitive design to allow CPOs to reduce their diagnostic overhead and maximise the uptime of their charging

network. When a charger connects to Switch, it uploads extensive diagnostics and performance data from the entire component structure of the EVSE (with OCPP 1.6 chargers, this is just the connector). It's like an MRIs scanner for the charging station: you can see everything, and manage everything now.

In this way, the Switch platform gives visibility to all sensor data of each component that a charging station manufacturer makes available. Through learning, predictive maintenance patterns can be established, resulting in fewer end-user failures and a better overall network performance. This, coupled with a customisable notification structure and different user profiles, allows the Charge Point Operator to manage their entire network remotely and only be alerted when there is a failure with a proposed resolution step.

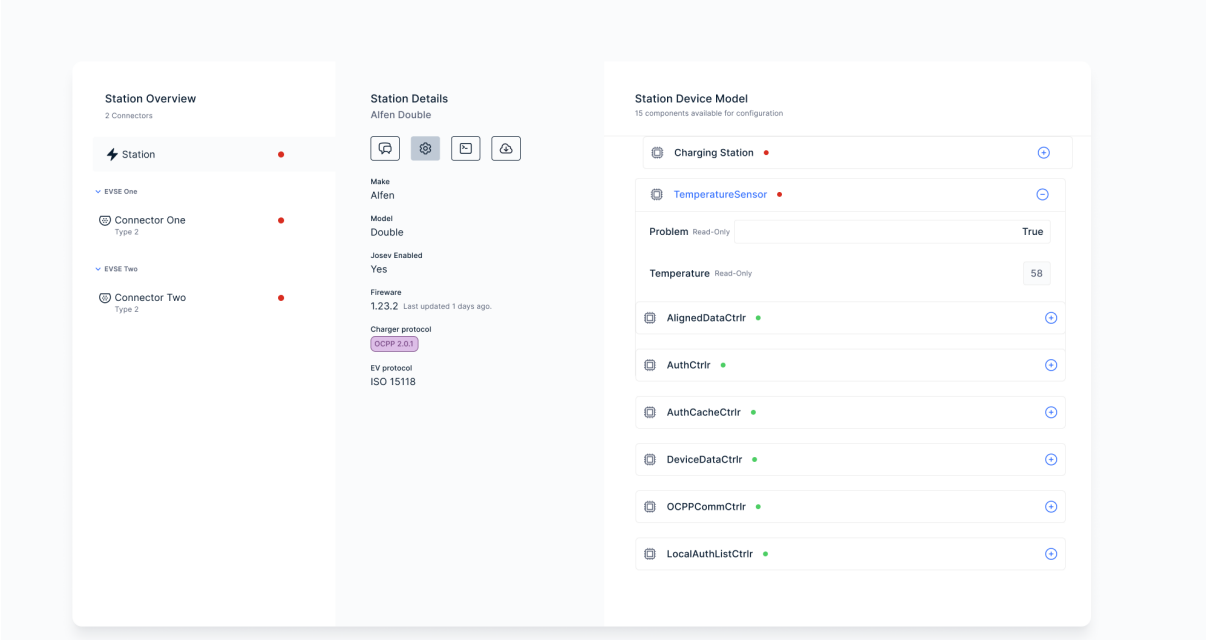

Fig. 12: The OCPP 2.0.1 'Device Model' (listing all components of a charger) visualised in the Switch platform

This is a first-to-market feature focused on maximising the uptime of your network and reducing your diagnostic overhead. You can cut the costs for maintenance staff in half as the technician doesn't need to visit the charger on site to figure out what's wrong. The Switch platform can tell you right away, based on the sensor data made available through the charging station. Ideally, using predictive maintenance, the CPO gets alerted when a charger component might fail due to past performance data. Switch will soon bring this predictive maintenance feature to market.

The Switch platform also addresses the topic of cost reduction and return on investment by partnering with the V2G and smart charging pioneer Nuvve. By offering operators the option to use smart charging algorithms to better manage their site load,

they avoid costly site upgrades. This, along with commercially scaled V2G technology allows network operators to maximise their value generation.

Reducing diagnostic overheads and upgrade costs, combined with a flexible tariff management (static and scheduled tariffs), allow you to fully monetise and grow your network at ease.

Provide ease of use

A focus on the user experience for both operator and driver is often undervalued within the industry. Switch has invested a significant part of the product build in creating a sophisticated and intuitive UI. This means that system operators don't need to be experts. We also prioritise essential features that drivers will sooner than later expect everywhere, such as Plug & Charge, which maximises the competitiveness of the operator by elevating their customers' user experience.

Switch provides a deeper visibility into the ISO 15118-based Plug & Charge conversation between the EV and the charger within our platform. This allows our customers to better analyse any potential issues that may arise during Plug & Charge sessions. So far, these sessions have been a complete black box with other CSMS providers. As mentioned in this paper, Plug & Charge is already becoming an expected feature for EV drivers regardless of the charging location. Switch has been at the forefront pioneering this technology, and can now support our customers in attracting more EV drivers and, thus, better monetise their charging network. Furthermore, the comprehensive data provided to car OEMs on their performance in the market with Plug & Charge significantly contributes to advancing and the industry delivering an improved charging experience all round.

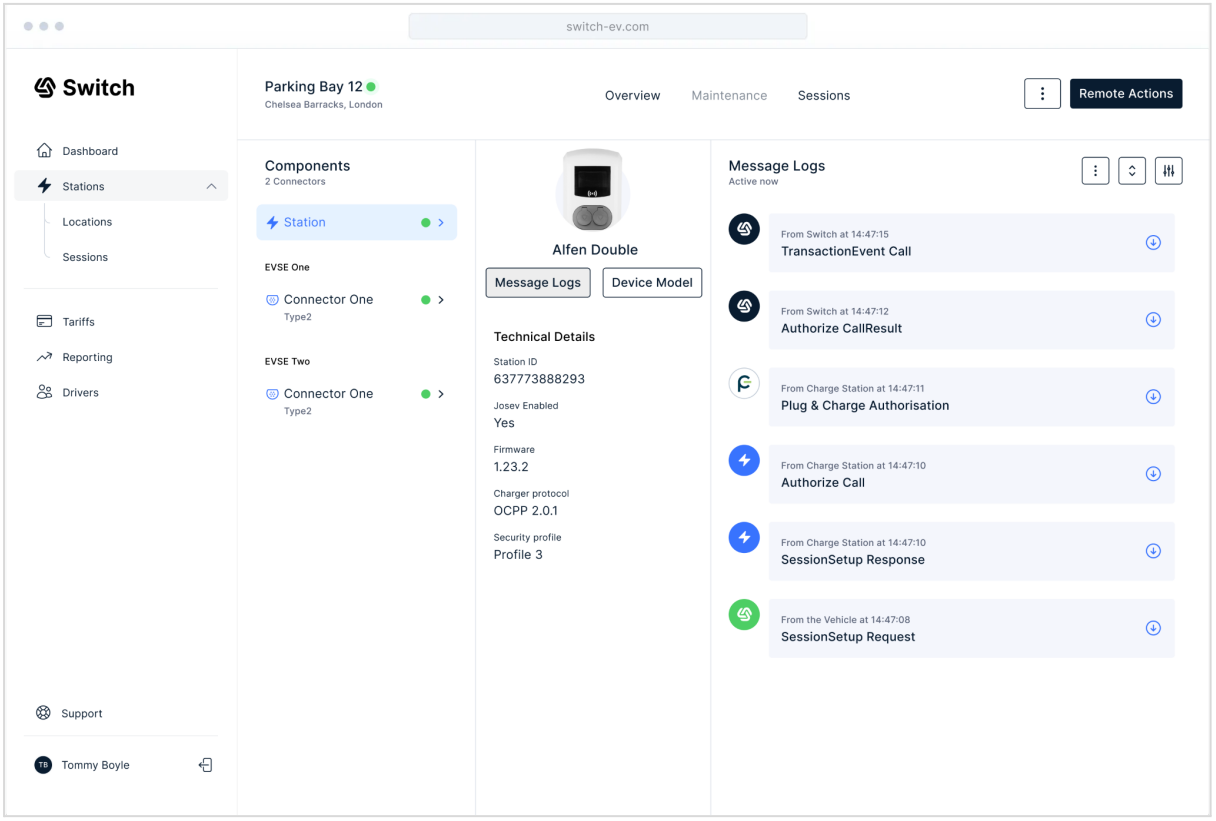

Fig. 13: Switch platform showing the message logs between EV, charger and the CSMS in a WhatsApp-like style. Message details support the CPO when debugging a faulted charging session.

Enable a seamless, vertically integrated solution

Being able to manage all supporting systems and processes, alongside EV charging, is an industry wide pain point. Switch addresses this by adopting an open API approach with its platform customers. This allows operators to integrate the Switch platform with existing systems and processes, such as ticketing and CRM systems, to better manage their network.

In terms of interoperability, Switch is constantly exploring to maximise interoperability across all parts of the value chain. The Switch platform is built on the industry standards OCPP 2.0.1, OCPP 1.6 and ISO 15118, which allows full-scale interoperability within the industry. Switch also supports the roaming protocols OICP (Hubject) and OCPI. In particular, an OCPI build enables seamless integration with other third party services, such as payment and customer support, so the value proposition to the operator becomes a lot stronger.

Whilst our platform is hardware agnostic, Switch has an in-depth testing programme in place with a number of charger OEMs for both OCPP 1.6 and OCPP 2.0.1. This

ensures a smoother integration between the charger and the Switch platform. The list of participants is growing by the month as businesses and networks move to gain OCPP 2.0.1 advantages, supporting Switch's interoperability in the market.

The most seamless charging experience, however, can be achieved when a charging station runs on our embedded OS Josev and connects to the Switch platform. Think of Josev as the Android for EV chargers. Charger OEMs should be able to focus on their core business, investing their resources in what sets them apart from their competitors. Implementing and maintaining complex and evolving communication protocols and standards like OCPP 2.0.1 and ISO 15118 shouldn't be any of their concerns. Just like laptop manufacturers don't reinvent the wheel and implement Bluetooth or WiFi themselves. They rely on third-party components from experts that have mastered these technologies. Why should it be any different in the e-mobility industry? With a decade of experience in interoperability testing, Switch knows all the corner cases and unique implementations in the field – so you don't have to.

Josev supports all relevant communication standards and comes with a well-defined API to help charger OEMs integrate this plug-and-play solution into their products.

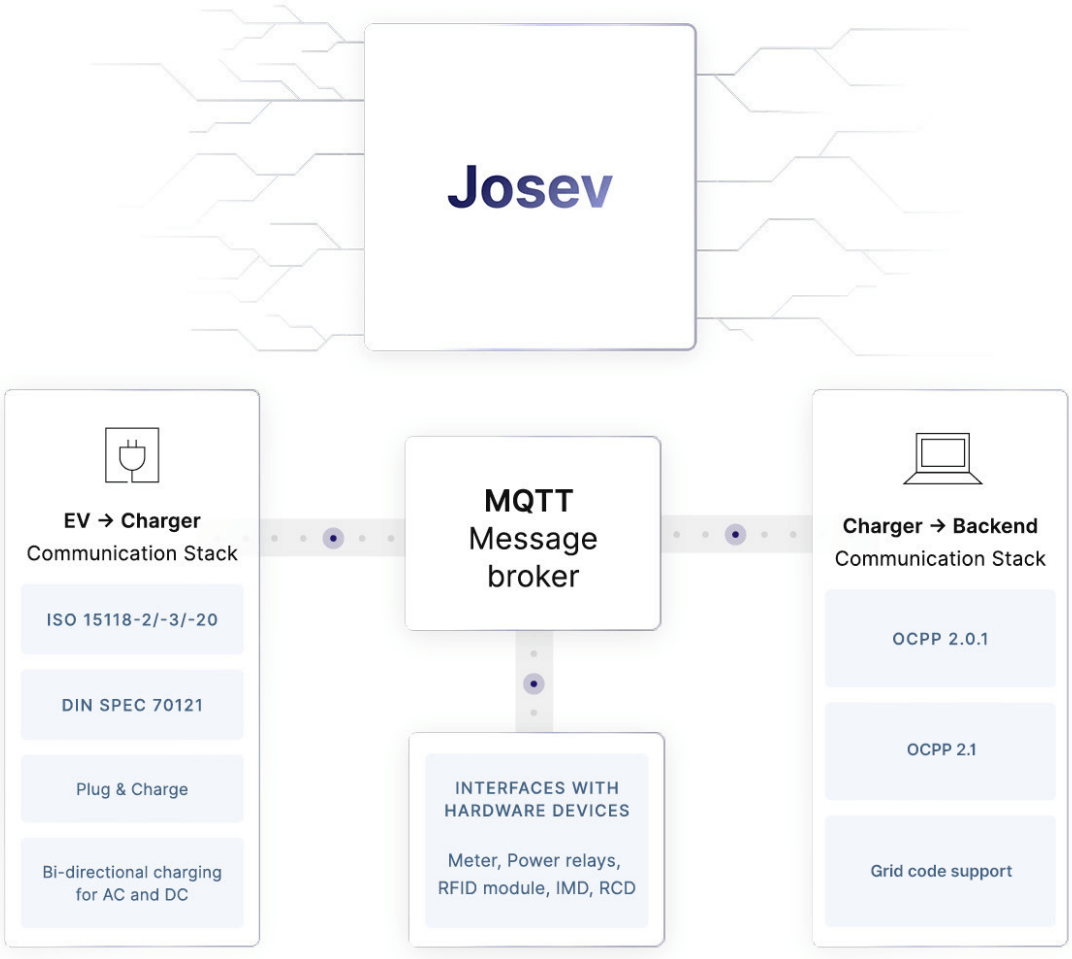

Fig. 14: The Josev Professional microservice architecture

Guarantee a future-proofed solution

The technology to build, scale and future-proof EV charging ecosystems with ease lies within the Switch platform and Josev. By offering an OCPP 1.6 based connection, operators can onboard their legacy charging infrastructure with us today and we will continue to collaborate with them over time. This allows operators to upgrade their network and unlock future expected capabilities, through our vertically integrated solution. Switch also offers protocol agnostic capabilities such as advanced reports, payment and billing solutions.

Enabling operator growth is a key part of our future-proofed solution. With this growth comes a need for maximum security. Chargers connected to the Switch platform on OCPP 2.0.1 benefit from the most secure connection possible using mutual TLS authentication and encryption so that both the charger and the platform are guaranteed to be safe. User data and other sensitive data is stored in a protected database secured by AWS. Other security threats are constantly monitored and mitigated using industry best practices. Our APIs incorporate multiple levels of access security applied and we actively protect against others such as SQL Injection and malicious packages using third party monitoring tools.

In June 2023, Switch will be among the first platforms globally to receive OCA certification for its OCPP 2.0.1 implementation. It puts us ahead of other charging management platforms due to our intuitive and future proofed technology.

In summary, the Switch ecosystem sets itself apart from the rest of the industry with its unique combination of a vertical integration of future-proof solutions (Josev and Switch platform) and strategic partnerships (Nuvve and chargebyte).

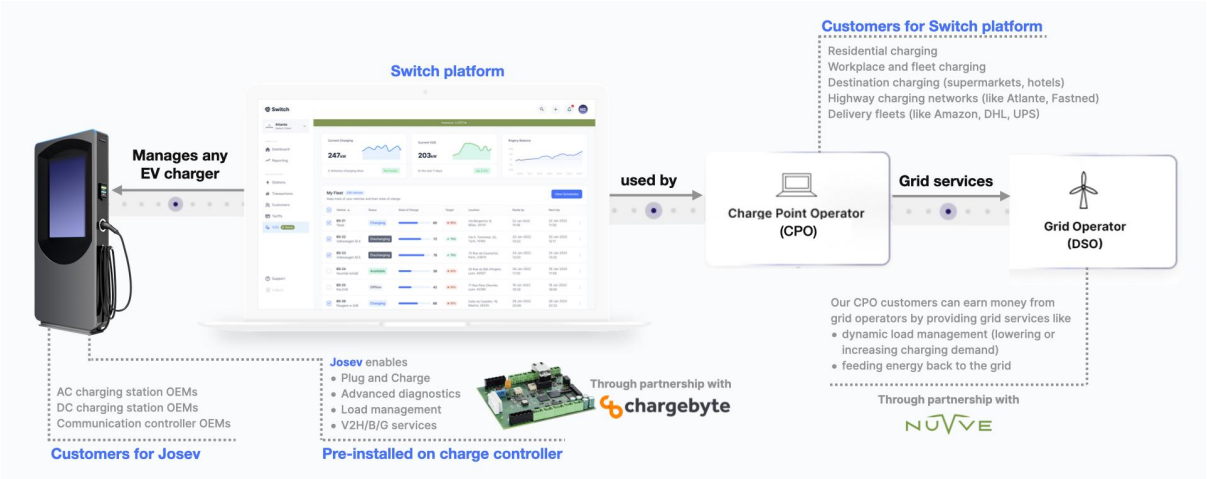

Fig.15: The vertical integration of the Switch ecosystem with its strategic partnerships

The Switch approach sets us apart from the competition. It enables us to support you in building superior EV charging networks that carry real market value and benefit your customers. With Switch, you gain a competitive advantage that pushes your business to the next level – so this will be the last Switch you'll ever make.

Abbreviations

The e-mobility industry loves abbreviations. Consider this section your handy cheat sheet that guides you through the jungle of terms used in this white paper and the wider industry.

AES – Advanced Encryption Standard
AFIR – Alternative Fuels Infrastructure Regulation

CA – Certificate Authority
CCB – Contract Certificate Bundle
CCP – Contract Certificate Pool
CCS – Combined Charging System
CN – Common Name
CP – Certificate Policy
CPO – Charge Point Operator
CPS – Certificate Provisioning Service
CSMS – Charging Station Management System

DER – Distinguished Encoding Rules
DH – Diffie-Hellman

ECC – Elliptic Curve Cryptography
ECDH – Elliptic Curve Diffie Hellman
ECDSA – Elliptic Curve Digital Signature Algorithm
EIM – External Identification Means
EMAID – E-Mobility Account Identifier
EV – Electric Vehicle
EVCC – Electric Vehicle Communication Controller
EVSE – Electric Vehicle Supply Equipment

HSM – Hardware Security Module

JOSEV – Joint Operating System for EV chargers

MAC – Media Access Control
MO – Mobility Operator (synonymous with MSP)
MSP – Mobility Service Provider (synonymous with MO)

OCPI – Open Charge Point Interface
OCPP – Open Charge Point Protocol
OCSP – Online Certificate Status Protocol
OEM – Original Equipment Manufacturer
OICP – Open Intercharge Protocol

PCID – Provisioning Certificate Identifier
PCP – Provisioning Certificate Pool
PFS – Perfect Forward Secrecy
PKI – Public Key Infrastructure
PLC – Power Line Communication
PnC – Plug & Charge
PWM – Pulse Width Modulation

RCP – Root Certificate Pool
RFID – Radio Frequency Identification
RSA – Rivest-Shamir-Adleman (the surnames of the inventors of this crypto algorithm)

SAE – Society of Automotive Engineers International
SECC – Supply Equipment Communication Controller
SHA – Secure Hash Algorithm
SLAC – Signal Level Attenuation Characterisation

TCP – Transmission Control Protocol
TPM – Trusted Platform Module
TLS – Transport Layer Security

V2G – Vehicle-2-Grid