Plug&Charge

State of the Industry Report 2023

Overview over the actual implementation of Plug&Charge in the global EV Industry

Publication date: 24 May, 2023

HUBJECT

On Hubject

Hubject simplifies the charging of electric vehicles.

With Plug&Charge, Hubject has created a service that allows Charging Point Operators (CPO), Mobility Operators (MO) and EV Manufacturers (OEM) to offer their clients a seamless and secure charging experience. To enable Plug&Charge services, Hubject operates their own V2G root Public Key Infrastructure, the Plug&Charge ecosystem and an open testing environment for both ISO 15118-2 and ISO 15118-20 standards.

Through its eRoaming platform intercharge the eMobility specialist connects Charge Point Operators (CPOs) and eMobility Service Providers (EMPs) to provide standardised access to charging infrastructure regardless of any network. Hubject has established the world's largest cross-provider charging network for electric vehicles by connecting CPO networks encompassing over 500,000 connected charging points and more than 1,250 B2B partners across 52 countries and four continents.

In addition, Hubject is a trusted consulting partner in the eMobility market, advising automotive manufacturers, charging providers, and other EV-related businesses looking to launch eMobility services.

In essence, Hubject promotes eMobility and its advancement worldwide. Founded in 2012, Hubject is a joint venture of the BMW Group, Bosch, EnBW, Enel X, E.ON, Mercedes-Benz, Siemens and the Volkswagen Group. Hubject's headquarters are in Berlin, with subsidiaries in Los Angeles and Shanghai.

We invite you to find more at hubject.com

For more information on Plug&Charge, please contact us as follows:

Web: https://www.hubject.com/plug-charge-ecosystem
Email: plugandcharge@hubject.com

The State of the Industry Report on Plug&Charge in 2023 was prepared by the Plug&Charge and Marketing department of Hubject, with contributions by Christian Hahn, Steffen Rhinow, Amit Bhonsle, editing by Carol Kacperski and design by Timo Weigelt.

The data and information was provided by Hubject GmbH.

For further insights and data, visit: https://www.hubject.com/ecosystem-overview

Index

1

Executive Summary

Plug&Charge is an industry-wide innovation that is actively changing the face of EV charging as it becomes the main method of authentication for EV drivers. With this inaugural Plug&Charge industry report, we are examining the progress of development, implementation and adoption of Plug&Charge, as well as the main trends and business perspectives that this innovative technology sets into motion within the eMobility industry.

This report shall help readers to form an advanced understanding of the developments in the industry and provide the foundations for stakeholders to formulate strategic decisions on how to implement this technology of the future.

Plug&Charge is an established solution that is set to become the status quo for authentication

Roles and responsibilities for Plug&Charge ecosystem operators and ecosystem participants have clarified.

Throughout 2022, the roles and responsibilities of Charging Point Operators (CPO), EV manufacturers (OEM), Mobility Operators (MO), Charging Point Manufacturers (EVSE OEM) as well as test labs have clarified. While the stakeholders within the Plug&Charge ecosystem reflect the plurality inherent in eMobility, at this mainstream stage the adoption of Plug&Charge hinges on the rollout of appropriate hardware and software by CPOs.

Shared market rules regarding Plug&Charge are emerging amongst discussions by eMobility stakeholders.

As Plug&Charge becomes the status quo of EV charging, all major stakeholders must agree on and finalise a set of critical market rules focused on interoperability, transparent governance, neutral V2G root CA operation, data protection and non-discriminatory contract-handling to ensure that the Plug&Charge ecosystem offers fair and equal treatment to all participants, as well as the integrity and stability of the eMobility industry overall.

While several ISO 15118-2 based solutions are in development, Hubject's Plug&Charge services became most widely adopted in the market.

Adoption of Hubject's Plug&Charge services, including the V2G PKI for the European, North American and Asian market, has seen a considerable increase throughout 2022. Major OEMs, CPOs and MOs have joined the Plug&Charge ecosystem and implemented Plug&Charge in their products.

There are several potential alternate solutions for ISO 15118-2 and -20 compliant PKI in development.

Plug&Charge is in a phase of mainstream adoption

A record-breaking number of Plug&Charge enabled EVs hit the roads in Europe and North America.

As more and more major OEMs signed on with Hubject to integrate Plug&Charge services into their electric vehicles (EV), the number of EVs equipped with Plug&Charge on the road quadrupled throughout the year, hitting a milestone of 100% growth from the third to fourth quarter. Major OEMs from Europe, North America and Asia are committed to providing a superior charging experience to their customers, and EV drivers now expect Plug&Charge services in their purchasing considerations.

The number of successful public charging sessions using Plug&Charge skyrocketed.

The rising number of Plug&Charge enabled EVs on the roads has a direct impact on the number of charging sessions. Throughout 2022, Hubject observed a rise in the number of public charging sessions using Plug&Charge. Between the second and third quarter, successful authorisations doubled, and remained steady for the last quarter of 2022, leading us to believe that EV drivers discovered the superior comfort of Plug&Charge and prioritised Plug&Charge capable networks for their public charging needs.

The number of Plug&Charge enabled EV charging networks grew as major CPOs signed on with Hubject.

An increasing number of CPO are responding to the demand of Plug&Charge capable public charging stations. 2022 was the year to commit to innovation for several major CPO players in eMobility. Electrify America, BP Pulse, Total Energy and MER have shown themselves as frontrunners in EV charging innovation by implementing Plug&Charge throughout their EV charging networks in record time. Aral, Ionity and Allego, all of whom have charging networks with great coverage, are currently in the process of onboarding to and rolling out their Plug&Charge services.

Plug&Charge meets the growing need for cybersecurityin the eMobility sector

Plug&Charge is set to replace traditional methods of authentication due to its higher level of cybersecurity.

Traditional methods to begin the public charging process, such as RFID, mobile apps, Mac Address based identification and credit cards have IT security weak spots. Any vulnerabilities in the end-to-end process can lead to potential safety hazards, privacy breaches, and financial losses for consumers and eMobility market players. Plug&Charge has established itself as the most secure authentication method for private and commercial use cases.

Plug&Charge is built on the automated exchange of asymmetrically encrypted certificates from trustworthy V2G root PKIs.

Public Key Infrastructures (PKI) ensure secure authentication and encryption and thus, secure communication between electric vehicles and charging stations. The digital certificates that are automatically exchanged upon plugging in the EV are asymmetrically encrypted using a private key and decrypted by the corresponding public key. This establishes trust in the authenticity and integrity of the information shared and makes the information inaccessible to third parties.

V2G root PKI operators must pass an information security audit in compliance to ISO 27001:2013 to prove quality and security of service.

V2G root PKI operators like Hubject need to clear an Information security audit in compliance with 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 organization. By passing this audit regularly, PKI operators can prove the quality and security of their processes to the eMobility industry.

Plug&Charge operators are ensuring interoperability between PKI, ecosystems and ISO standards

Plug&Charge ecosystems must prevent lock-in and ensure interoperability by integrating multiple, non-proprietary V2G root PKI.

2022 has shown that interoperability is key. Plug&Charge operators must ensure multi-PKI interoperability within their ecosystems. The integration of multiple V2G root PKI into a Plug&Charge ecosystem is critical for the expansion and integration of EV charging infrastructure, ensuring convenience, accessibility, and security for all stakeholders in eMobility. Non-proprietary V2G root CA operators will mitigate potential lock-in effects and enhance flexibility for all ecosystem participants.

When multiple ecosystems become available, multi-ecosystem interoperability will become prerequisite for a seamless EV charging experience.

Multi-ecosystem interoperability has become a topic of interest in 2022. Hubject has tested their ecosystem in collaboration with ElaadNL with the goal of preventing future incompatibilities for current clients. Interoperability between ecosystems was possible when using the Open Plug&Charge Protocol. A non-proprietary protocol that will be backwards compatible with the OPCP is currently under discussion by a governance group connecting all relevant stakeholders of the EV industry to ensure standardised communication between ecosystems in the future..

With ISO 15118-20 available, Plug&Charge ecosystems must manage a smooth transition between standards to ensure interoperability.

Solutions based solely on the new ISO15118-20 norm will be implemented in the market over the next few years. For the interim period of transition, it is essential for the Plug&Charge ecosystem to be able to support both norms at the same time to ensure the best possible interoperability. Hubject's Plug&Charge solution will provide a smooth transition for all stakeholders between the ISO 15118-2 and 15118-20

2

State of the Industry in 2023

The adoption of Plug&Charge as the international standard for the EV industry can be differentiated into three phases: development, deployment, and mainstream adoption.

During the first development phase from 2014 to 2019, a handful of pioneering companies collaborated to create the technical specifications for Plug&Charge functionality. This laid the foundation for the deployment, the second phase, during which the first electric vehicles and charging stations with Plug&Charge functionality were launched, and early adopters began using it.

Currently, the market is in the mainstream adoption phase, which means that most car manufacturers and charging point operators are incorporating Plug&Charge technology into their products.

Furthermore, organizations worldwide are evaluating the potential of ISO 15118-20, the international standard that sets the basis for the secure information exchange required for a more secure and customer friendly authentication.

Despite this, there are currently one productive and several emerging Plug&Charge solutions available on the market. As technology continues to evolve and gain widespread adoption, we can expect to see a growing diversity in approaches to ISO 15118-2 and –20 solutions, and further advancements in technology to improve its functionality and security.

2.1 Ecosystem Roles

The stakeholders within the Plug&Charge ecosystem reflect the plurality inherent in eMobility.

Many industry players are already implementing Plug&Charge or have committed to implementation on their business roadmap. Charging point operators (CPOs), automotive manufacturers (OEMs) and charging equipment manufacturers, as well as eMobility providers are leading the adoption process. In the following, we have delineated their roles and responsibilities in the Plug&Charge ecosystem:

Ecosystem Player	Roles & Responsibilities
Charging Point Operators (CPOs)	CPOs are staying ahead of the curve by providing EV drivers with charging networks that support Plug&Charge. Accessibility, usability and perception of public EV charging rely on the quality of infrastructure provided by CPOs. Therefore, the adoption of Plug&Charge hinges on the rollout of appropriate hardware and software. By deploying chargers that support Plug&Charge and implementing the functionality on their backend system, CPOs create a strong touchpoint for EV drivers looking for the best possible charging experience.
Automotive Manufacturers (OEMs)	Automotive OEMs are critical to the establishment of a thriving Plug&Charge ecosystem, as they bring the electric vehicles (EVs) to market. The implementation of Plug&Charge requires specific hardware and software in the EV Charge Controller, the component in the electric vehicle that controls charging of the battery. Following user-demand, Auto OEMs like VW, Ford and BMW have invested in this development and successfully integrated Plug&Charge into their EVs. Plug&Charge enables “Multi-Contract Handling”[1], a feature that provides drivers with the flexibility to switch between multiple contracts in their EV and choose based on different use cases.
Mobility Operators (MOs)	MOs serve as the bridge between the charging point and the EV driver by providing the digital charging service to the EV driver. The MO is instrumental in the authentication process between the EV and the charging station. To handle authentication via Plug&Charge, payment authorization and processing, the MO’s backend needs to be integrated in the Plug&Charge ecosystem.
Charging Point Hardware Manufacturers (EVSE OEMs)	Charging point hardware manufacturers invest in developing charging stations that conform to the ISO 15118 –2 and/or the ISO 15118-20 standard. The hardware and software in the charging point must support Plug&Charge, which requires testing and certification.
Test Labs	Test Labs facilitate end-to-end testing with official V2G Root certificates. This ensures interoperability and mitigates lock-in effects caused by proprietary testing. As of 2022, there are not enough test facilities available that are equipped to support Plug&Charge testing.

[1] For further information on Multi-Contract Handling, see our section in chapter 5.2.

2.2 Market Rules

It is vital for the integrity and stability of the eMobility industry at large that all those involved in the development and implementations of new and innovative solutions such as Plug&Charge keep to not only international standards like ISO 15118-2, but to a number of emerging Market Rules.

As Plug&Charge is set to be the status quo of EV charging, there is vested interest by all stakeholders that the growing Plug&Charge ecosystem be fair and equal. In the following, we have outlined several key topics that are deserving of discussion to ensure healthy collaboration and competition within the eMobility ecosystem.

Interoperability	V2G Root PKI should not be tied to ecosystems, and ecosystems should not run on a single V2G Root PKI. Every stakeholder using Plug&Charge should be able to use any V2G Root of their choosing. To enable this level of interoperability between different root CAs, we must ensure that all PKI and ecosystem operators meet a minimum level of requirements regarding IT Security. This minimum should be certified by external auditing organizations.
Transparent Governance	Information on the operational processes of any V2G Root CA must be publicly accessible. Ideally, market players should be able to download the certificate policy and other relevant documents easily from the operator's website. To aid understanding, these documents should be supported by additional information regarding external security audits. Transparent governance ensures that all market players act on a level playing field. Open access to information promotes innovation and leads to the best possible outcomes for end-customers.
Neutral Root CA Operators	As the V2G Root Certificate Authority is a mandatory requirement to enable Plug&Charge, we must consider whether providing access to the V2G Root Certificate should be a business service or a mandatory requirement for ecosystem operators.
Data Protection	To build trust and integrity as the Plug&Charge ecosystem grows, PKI operators have a duty to ensure data protection for end-customers and ecosystem participants. Plug&Charge services are based on Contract Certificates that are generated and issued by the MO through a V2G Root PKI and installed in the EV. These certificates carry both user information as well as sensitive information, as defined by the European GDPR, about direct competitors. The definition of sensitive information is not standardised on a global level, which adds further complexity. To ensure data protection, we must agree on shared standards and improve the encryption of this data to limit third-party access.
Non-discriminatory Contract Handling	To ensure nondiscriminatory access for services such as Plug&Charge, all EVs should support the installation of contract certificates based on driver preference. OEMs as well as MOs should support Multi-Contract Handling. The installation, update, removal or prioritization of an MO contract in the EV must be defined to give full control to the EV driver.

2.3 Plug&Charge Solutions

Active Solutions

— The Plug&Charge Ecosystem and V2G Root PKI by Hubject

Hubject, an eMobility company offering a range of services to the industry, is best known as the facilitator of the largest international eRoaming network. Hubject has led several successful Consulting and Research & Development initiatives that have been pushing for innovation across the industry.

Since 2019, Hubject has been operating a V2G-PKI and a service-based Plug&Charge Ecosystem. The solution is based on the industry recognized standards, ISO 15118-2 and VDE-AR-E 2802-100-1. Since then, an ever-increasing number of partners have adopted the standard and implemented Plug&Charge using Hubject's V2G-PKI[2] and Plug&Charge ecosystem[3]. Currently, Hubject operates the only V2G Root Certificate Authority that serves as the trust anchor to ensure a secure certificate exchange and enable Plug&Charge. The company is committed to continuously developing their Plug&Charge functionality to offer a futureproof solution to their ecosystem partners.[4]

2022 also saw the launch of the first V2G root PKI for ISO 15118-20, and its integration into Hubject's open Plug&Charge testing environment, which has since become the system to use for multi-standard interoperability testing.

As a member of different international organizations, Hubject has been instrumental in developing the technical specifications for Plug&Charge, and was the first to develop a functioning Plug&Charge solution. 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.

Hubject offers easy and standardized onboarding, smooth technical integration and a comprehensive range of testing and validation possibilities for each stakeholder's individual use case.

Solutions in Development

— "Plug & Charge Europe" by CharIN

CharIN, short for Charging Interface Initiative, is a global association of eMobility. The goal of the project is to set up a V2G Root CA with CharIN as the operator and provider of required services.[5]

In September 2022, the CharIN PKI was set up for production in collaboration with security company Irdeto.[6] CharIN showcased the integration of their PKI on a research level with Gireve.[7] CharIN has tentative plans to publish a PKI for the new ISO 15118-20 standard.

— Plug and Charge Services by Gireve

French eRoaming platform provider Gireve has pledged to operate its own V2G-Root PKI and establish PKI services in collaboration with digital security company, Thales.[8] While Gireve has participated in tests using a prototype of their ecosystem[9], no further information on a release of their solution has been provided. No timeline of their Plug&Charge project has been publicly disclosed.

— "Electric Vehicle (EV) Charging Public Key Infrastructure (PKI)" project by SAE International

Society of Automotive Engineers (SAE) International, a professional association and standard development organization based in the United States, has focused on eMobility. SAE has launched an industry-led pre-competitive research project alongside Eonti, DigiCert and VerSprite in May 2020.[10] In April of 2022, SAE tasked its technical contractors to first test the SAE EV charging PKI.[11] As of yet, there is no public information available on the progress of their project.

[2] For Hubject's PKI, visit https://www.hubject.com/download-pki

[3] To see Hubject's ecosystem, please visit https://www.hubject.com/ecosystem-overview

[4] https://www.hubject.com/blog-posts/hubjects-plug-charge-team-is-first-to-launch-iso15118-20-public-key-infrastructure-in-their-free-testing-environment

[5] https://www.charin.global/media/pages/news/plug-and-charge-europe-enabled-by-charin-is-soon-to-be-rolled-out/42fa18766d-1618926195/press-release-plug-and-charge-europe.pdf https://www.charin.global/news/plug-and-charge-europe-enabled-by-charin-is-soon-to-be-rolled-out/

[6] https://www.charin.global/news/europe-is-ready-to-further-roll-out-plug-charge/

[7] https://www.gireve.com/gireve-plugandcharge-services-open-to-charin-v2g-pki/

[8] https://www.gireve.com/safe-ev-charging-for-user-experience-plug-charge-gireve/

[9] https://www.gireve.com/pool-interoperability-plug-charge-gireve/

[10] https://www.electrichybridvehicletechnology.com/news/charging-technology/ev-charging-security-project-gathers-pace.html

[11] https://www.sae.org/news/press-room/2022/04/sae-international-performs-first-test-of-ev-charging-pki-design

Key takeaways

Plug&Charge is well on its way to be the international standard of charging authentication for the eMobility industry. In 2022, Plug&Charge services truly reached the momentum of mainstream adoption, as OEMs and CPOs are incorporating Plug&Charge services into their products. However, only one productive Plug&Charge solution is currently available on the market, which is operated by Hubject. We can expect to see more Plug&Charge solution providers emerge as the technology evolves and gains widespread adoption.

Due to the increased rate of adoption, the roles and responsibilities of all the different stakeholders in the Plug&Charge ecosystem, including Charging Point Operators (CPOs), Automotive Manufacturer (OEMs), Mobility Operators (MOs), Charging Point Hardware Manufacturers (EVSE OEMs), and Test Labs have clarified. These stakeholders take on a variety of tasks, including providing charging networks that support Plug&Charge, bringing electric vehicles equipped with Plug&Charge to market, serving as a bridge between the charging point and the EV driver by providing Plug&Charge capable digital charging services, and investing in developing charging stations that are Plug&Charge tested and verified.

As the market for Plug&Charge expands, several key topics, such as interoperability, transparent governance, the neutrality of Root CA operators, and data protection, are vital for ensuring healthy collaboration and competition within the eMobility ecosystem. All major stakeholders must agree on and finalise a set of critical market rules on these topics to ensure not only fair and equal treatment for all Plug&Charge ecosystem and V2G root PKI operators and their partners, but also the integrity and stability of the eMobility industry overall.

3

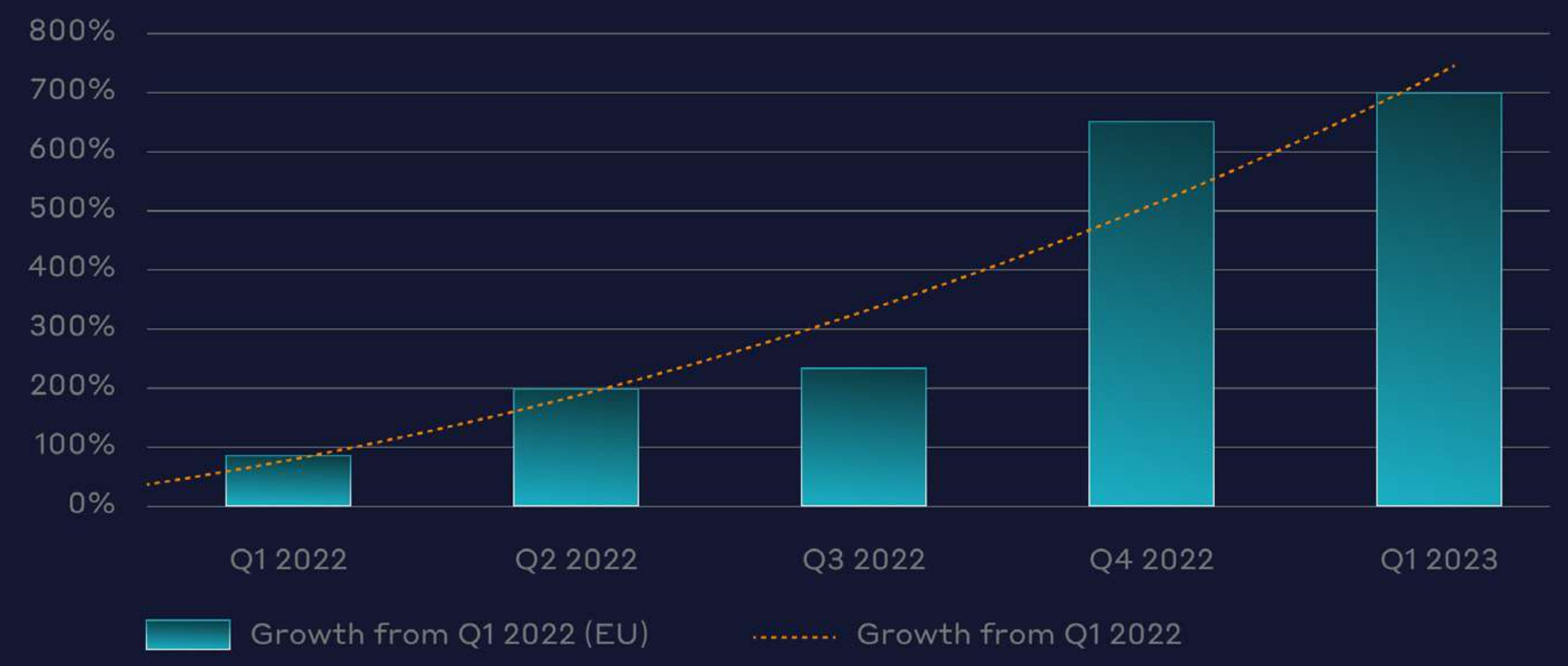
Ecosystem Growth

The push for Plug&Charge adoption originates from a variety of sources. Because consumers desire charging solutions on par with the relative simplicity of refuelling an internal combustion engine vehicle, EV manufacturers are motivated to adopt the technology to provide an improved user experience. Buying into innovative technology early also sets their vehicles apart from competitors, impacting the bottom line significantly.

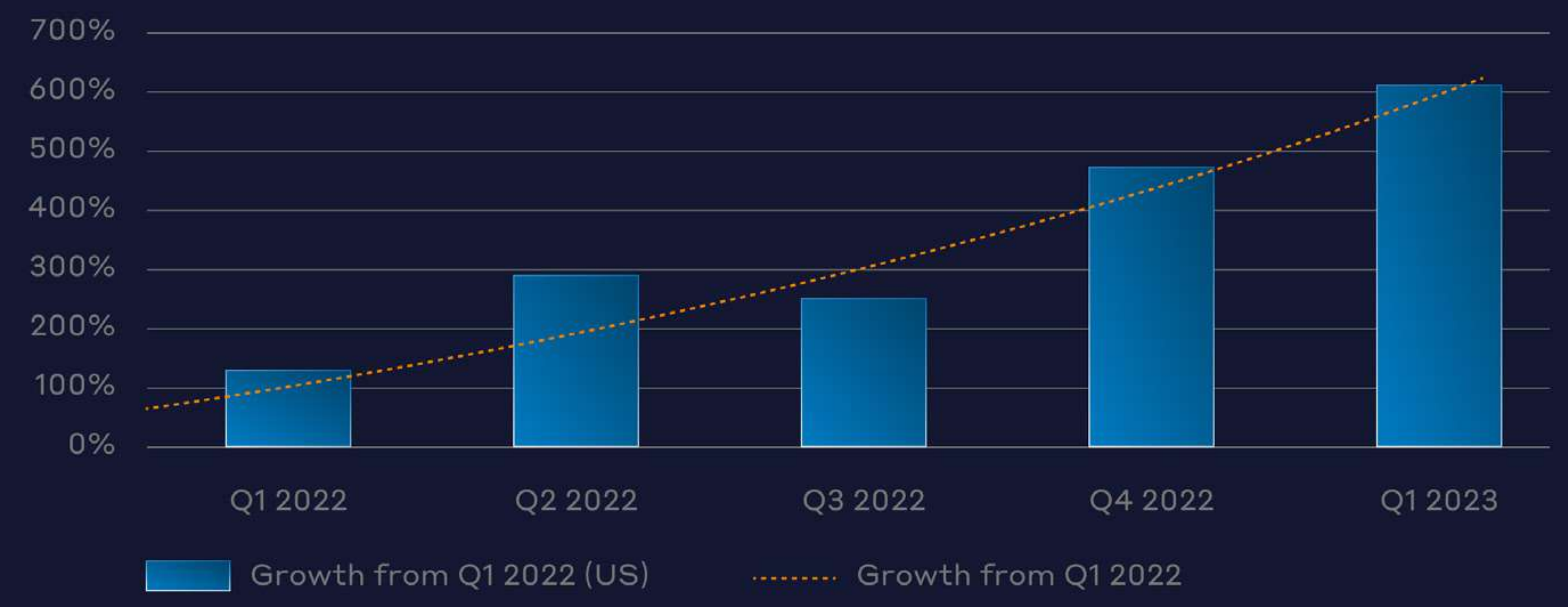
eMobility providers work closely with EV manufacturers to set up touchpoints with EV drivers that make driving an EV a breeze. Charging point operators are rolling out Plug&Charge in their networks to attract drivers and offer this seamless charging experience.

To review the growth of the Plug&Charge ecosystem throughout 2022, we must therefore look at each stakeholder's role individually. The number of Plug&Charge capable EVs on the road shows not only the development of Plug&Charge capable EVs but also their usage by EV drivers. Throughout 2022, EV manufacturers have enabled Plug&Charge in several new EVs to meet customer demand. We estimate that by 2030, all new EVs entering the market will be Plug&Charge capable, while legacy vehicles may be upgraded retroactively.

Growth Rate for Plug&Charge Contract Pool in the EU



Growth Rate for Plug&Charge Contract Pool in the US



EV drivers are adopting quickly to the effortless charging experience provided by Plug&Charge. Authentication rates throughout 2022 reveal impressive growth, cementing the fact that Plug&Charge is no longer in development and is now in a phase of mainstream adoption. The rapidly rising number of authorisations also shows the growing amount of Plug&Charge enabled charging stations.

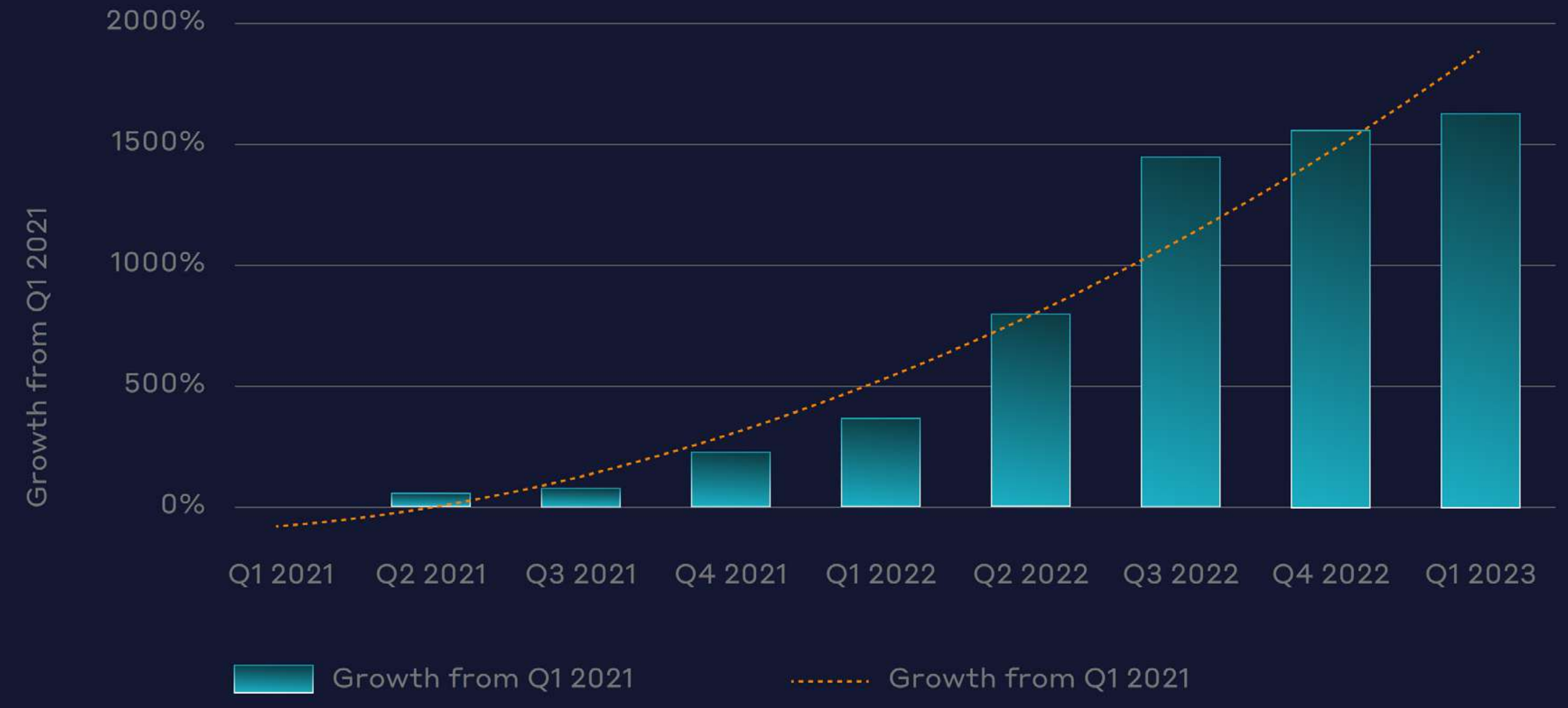
While the number of charging networks supporting Plug&Charge is still limited in 2022, an increasing number of CPOs are prioritizing Plug&Charge in 2023, driven primarily by the volume of vehicles from auto OEMs coming on the road and market regulations mandating Plug&Charge for standardization and interoperability. Performance, security, and maintenance of their charging network is currently of higher priority for many CPOs and upgrading existing hardware and implementing new software is both time-intensive and expensive. However, CPOs are already investing in Plug&Charge capable hardware to prepare for the moment that Plug&Charge becomes the status quo method of starting a charging session. The CPOs with Plug&Charge have experienced an increase in brand-recognition and customer loyalty as EV drivers discover Plug&Charge on the road.

The Plug&Charge ecosystem is reaching a tipping point in terms of adoption. As car manufacturers roll out EVs and eMobility service providers launch services with Plug&Charge, we expect charging point operators to follow suit and deploy ISO 15118-2 and ISO 15118-20 on their networks in 2023.

Several charging point operators are already in the onboarding process with Hubject's Plug&Charge team to enable the solution as soon as possible: TotalEnergies, Aral, Ionity and Allego, who all have established charging networks with great coverage over the past years are currently in the process of their operational onboarding. Accounting for the current growth rate, the rollout of Plug&Charge ready infrastructure is set to more than double (or triple) by the end of 2023.

Nonetheless, awareness of the factors driving and hindering the mass adoption of Plug&Charge functionality is vital to all stakeholders in the eMobility ecosystem. It is important to keep up with these developments to ensure that charging infrastructure remains futureproof and meets the needs of EV drivers for a safer and smarter way to charge their EV.

Plug&Charge Authorizations Growth Rate



Hubject is establishing the global Plug&Charge ecosystem

— Participants of the Hubject PnC-Ecosystem using the Hubject V2G Root

EV Producers (OEM)

CUPRA
KIA
PORSCHE
BMW GROUP
MINI
Ford
VINFAST
HYUNDAI
MAN
SCANIA
Mercedes-Benz
SKODA
GENESIS
LUCID

Charge Point Operator (CPO)

mer Pure energy from Statkraft
Longship.io
VIRTA
SMART/LAB
blink
PORSCHE
electrify america
electrify canada
Shell Recharge
driivz
zunder Charging Hero
IONITY
bp pulse
IBIL TECNOLOGÍA Y SERVICIOS DE RECARGA
TotalEnergies
BayWa
BOSCH
e·on
COMPLEO
Allego
Switch
sdey Syndicat Départemental d'Énergies de l'Yonne
has·to·be eMobility
EVGATEWAY

Mobility Operators

DIGITAL CHARGING SOLUTIONS
octopus ELECTROVERSE
Plugsurfing
SMART/LAB
e·on
Ford
VIRTA
BOSCH
IBIL TECNOLOGÍA Y SERVICIOS DE RECARGA
Elli
nOR+He
DEFTPOWER
PORSCHE
chargecloud

Charge Point Manufacturers (EVSE)

TRITIUM
intech
Porsche Engineering driving technologies
hypercharger by alpitronic
ALFEN
Zaptec
eSYSTEMS A KATEK Brand
ebee Part of Bender
BTC POWER
ABB

Source: hubject.com

4

Cybersecurity: Plug&Charge for a safer eMobility ecosystem

With the increasing adoption of electric vehicles (EVs), the development of easily accessible and secure charging ecosystem for EVs is becoming a top priority. EV charging infrastructure is a crucial interface point between the EV industry, consumers, and electric utilities.

Therefore, it is imperative that charging transactions are secure and trusted to ensure the seamless functioning of the eMobility ecosystem.

Any vulnerabilities in the end-to-end process can lead to potential safety hazards, privacy breaches, and financial losses for consumers and eMobility market players. Therefore, security and trust are at the forefront of the development of charging solutions.

Some wide-spread methods of managing the authentication at the charging station have been found lacking. RFID, apps, Mac Address based identification and credit cards are commonly used to authenticate when charging in public. However, all these methods have IT security weak spots that can be preyed upon:

- RFID cards can be easily copied or cloned, potentially leading to unauthorized access and security breaches as well based on the widely adopted MI Fare Classic and desfire standard[12] – using more secure RFID cards would require stakeholders to update the physical readers at charging stations.
- Apps typically require users to enter their login credentials to access charging stations and initiate charging. If these login credentials are not strong enough or if the user's device is compromised; attackers may gain access to the user's account and use it to initiate unauthorized charging or access sensitive information.
- Credit cards were not designed for authentication purposes and do not offer the same level of security and convenience as Plug&Charge. They are vulnerable to fraud, identity theft, and other security issues due to the vulnerability of the credit card information shared during the transmission necessary to initiate the charging process. Using pin pads will partly solve this problem but reduces customer convenience.
- Autocharge is a fully proprietary technology that relies on an EVs charge controller identifier to initiate and authorize charging, which can be easily spoofed or manipulated. This can lead to unauthorized access to charging stations, data breaches, and potentially dangerous situations.

[12] External web link (identbase.de)

Currently the most secure way to charge an EV at a public charging station is Plug&Charge, a technology that enables automatic authentication and charging of EVs without any human intervention. Given the sensitive nature of this step in the charging process, cybersecurity is of utmost importance.
To ensure secure communication between electric vehicles and charging stations, ISO 15118-2 has established a set of guidelines to ensure the secure information exchange needed for successful authentication in the Plug&Charge ecosystem.

In this ecosystem, digital certificates and public key infrastructures (PKIs) play a vital role in ensuring secure communication between electric vehicles and charging stations.

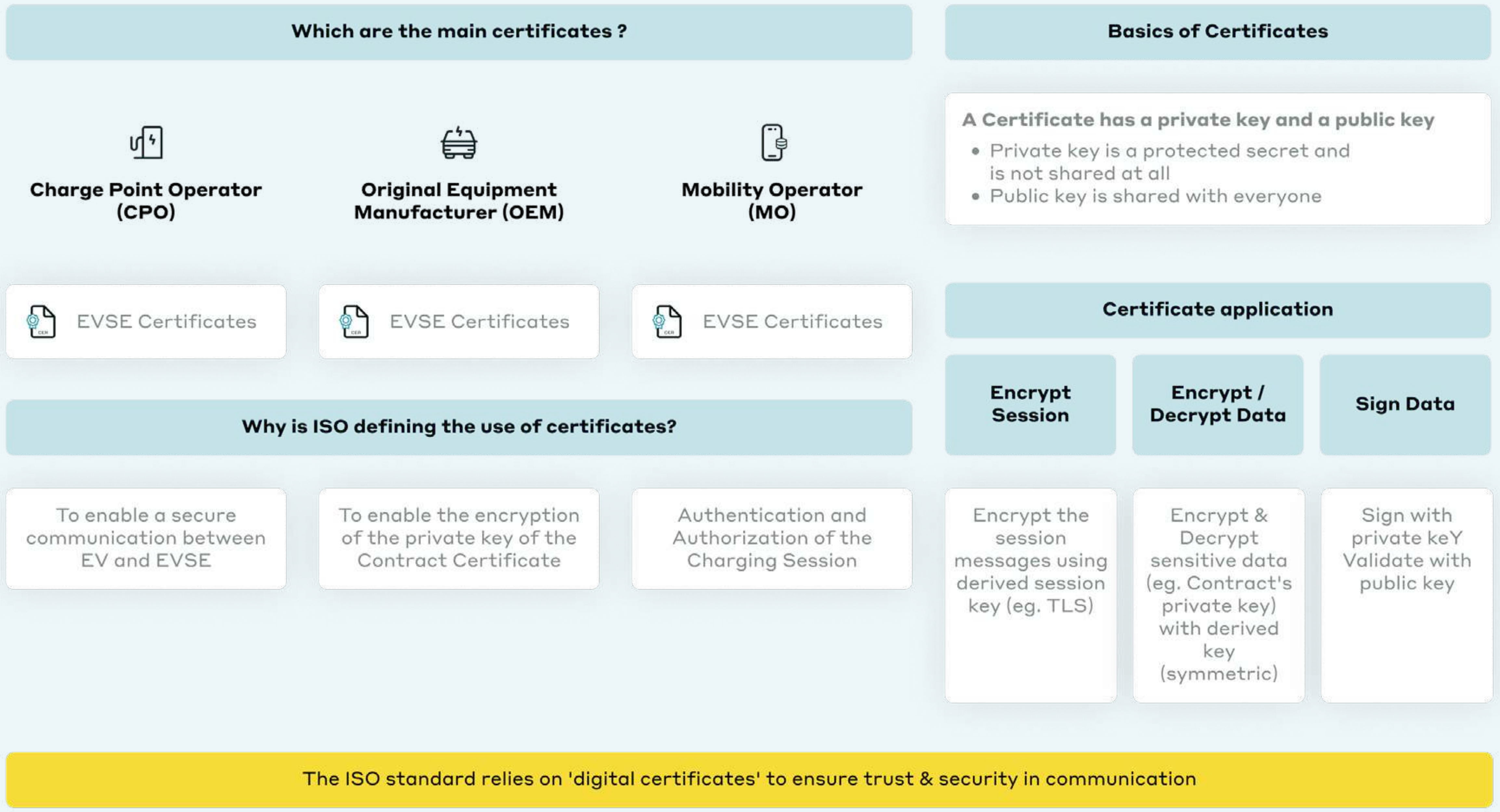
ISO 15118-2 defines the digital certificates that are required for secure information exchange between the EV and the charging station. These digital certificates are issued by public key infrastructures (PKIs), which are hierarchical structures of trusted certificate authorities (CA). The certificate authority acts as a trusted third-party 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.

A digital certificate is an electronic document that verifies the identity of an entity. It is also known as a public key certificate, and its authenticity is bound to a digital signature. Digital signatures are asymmetrically encrypted using a private key and decrypted by the corresponding public key, which establishes trust in the authenticity and integrity of the information shared.

The V2G-PKI is defined in the ISO15118-2 standard. With the V2G PKI, each member of the Plug&Charge ecosystem can generate specific certificates, sub-certificates, and leaf certificates that are bound to their role in the ecosystem. The V2G Root Certificate Authority (CA) is the highest trust point and is necessary to issue leaf certificates for Charging stations and for CPS-Services. A MO Root CA can by created individually by Mobility Operators and similarly, an OEM Root CA can be created by car manufacturers. All these Certificate Authorities (CAs) issue sub-certificates that are used for different purposes as defined in the ISO standard and VDE application guide.

Communication with Certificates

— There are different certificates per Use Case Group



Which are the main certificates ?

Charge Point Operator (CPO)

Original Equipment Manufacturer (OEM)

Mobility Operator (MO)

EVSE Certificates

EVSE Certificates

EVSE Certificates

Why is ISO defining the use of certificates?

To enable a secure communication between EV and EVSE

To enable the encryption of the private key of the Contract Certificate

Authentication and Authorization of the Charging Session

Basics of Certificates

A Certificate has a private key and a public key

- Private key is a protected secret and is not shared at all
- Public key is shared with everyone

Certificate application

Encrypt Session	Encrypt / Decrypt Data	Sign Data
Encrypt the session messages using derived session key (eg. TLS)	Encrypt & Decrypt sensitive data (eg. Contract's private key) with derived key (symmetric)	Sign with private keY Validate with public key

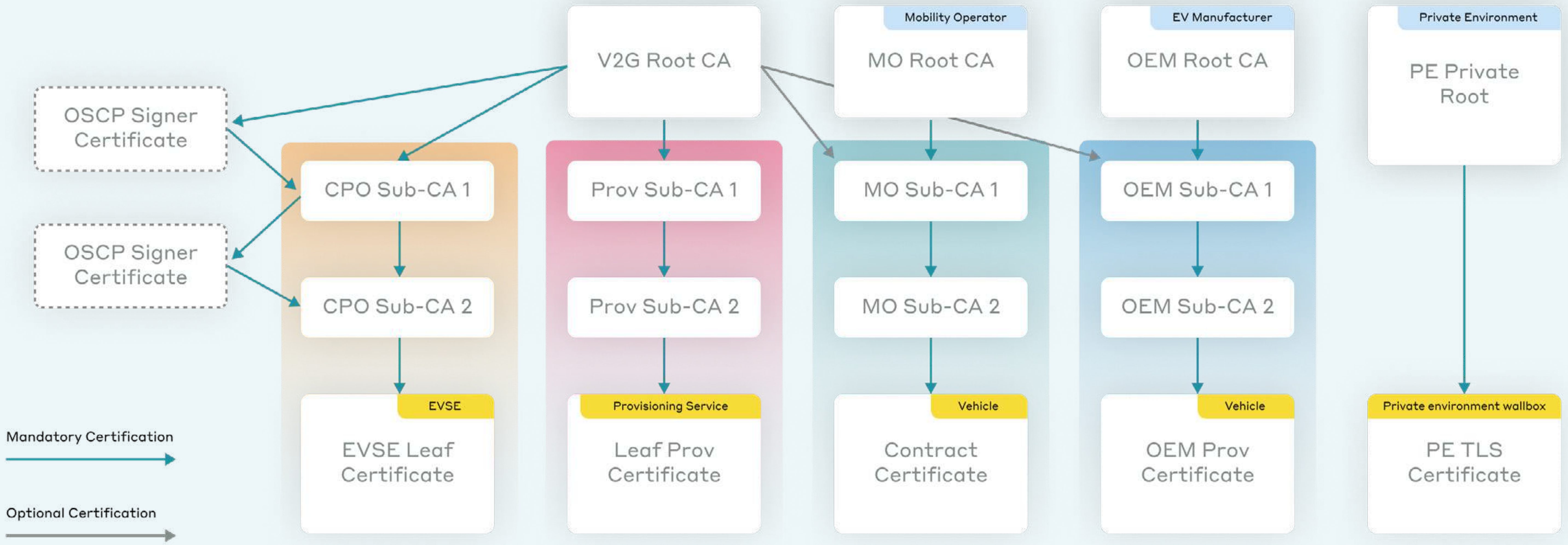
The ISO standard relies on 'digital certificates' to ensure trust & security in communication

All certificates are generated by PKIs and used and stored in Plug&Charge ecosystems. At this time, the Hubject Plug&Charge ecosystem is the central certificate storage, as no other ecosystems have entered the market.

Using public and private keys to asymmetrically encrypt certificates, storing these certificates in a shared ecosystem ensures interoperability but also security and trust across the eMobility ecosystem. At this time, Hubject operates the V2G-Root PKI that provides all ISO1511-2 SubCAs.[13]

Public key infrastructure for each P&C market role as outlined in ISO 15118

— One PKI for each Plug and Charge market role



Charge Point Operator (CPO)
Operates and maintains the charging stations via its backend IT system

Certificate Provisioning Service (CPS)
Facilitates the installation of a new contact certificate for the EV through digital signature

Mobility Operator (MO)
Provides a legal e-mobility contract and issues contract certificates associated with that legal contract

Car manufacturer (OEM)
Issues the unique OEM provisioning certificate needed to install a new contract certificate for Plug&Charge

Source: *https://www.iso.org/standard/55366.html*

[13] All information on these certificates can be found in Hubject's Certificate Policy.

Currently, Plug&Charge is considered the most secure method for authenticating the charging process of electric vehicles on the market adopted by the industry. However, like any technology, it is not perfect, and there are still areas that need improvement.

While Plug&Charge has eliminated some of the problems associated with manual authentication methods, such as RFID cards, credit cards, and mobile applications, there are still aspects of the technology that require attention to ensure its bulletproof security.

Nonetheless, as the technology continues to evolve, ongoing efforts must be made to improve its security and reduce any potential vulnerabilities.

Market Rules: Data Security according to ISO 27001:2013

To prove the integrity of its V2G root PKI operation procedures, Hubject underwent an audit in 2020, in compliance with ISO 27001:2013, an international standard that outlines the requirements for establishing, implementing, maintaining, and continuously improving an information security management system within the context of an organization.[14] This certification must be renewed every three years to ensure the consistent upkeep of security standards. Furthermore, Hubject partners with an information security company, Nexus Group, that is an established expert in operating Public Key Infrastructures.

By meeting the standard's ISO 27001 requirements, Hubject shows its commitment to cybersecurity and confirmed its ability to implement exceptional data privacy, identity management, and security standards. The ISO 27001:2013 certification serves as an affirmation of Hubject's dedication to information security and assures its customers and partners that their sensitive information is protected.

To additionally showcase transparency and encourage information access to its PKI operation procedures and best practices for parties interested in the technical specifications of their Plug&Charge services, Hubject publishes its Certificate Policies for the European, US and Asian PKI on the Hubject website: https://www.hubject.com/download-pki

[14] https://assets.website-files.com/602cf2b08109ccbc93d7f9ed/636275f45e72fadc738ad38d_Hubject%20ISO%2027001%20Audit%20Certificate.pdf

4. Cybersecurity: Plug&Charge for a safer eMobility ecosystem

Market recommendation

To ensure that the eMobility industry meets cybersecurity demands, stakeholders in the Plug&Charge industry must develop a set of market rules to govern audits and interactions. Plug&Charge providers and V2G root PKI operators should seek a verification of their information security setup through a third person audit that meets international standards. Additionally, V2G root PKI operators as well as Plug&Charge providers must take care to collaborate with companies that have passed the necessary information security audits. We expect that these developments will go hand in hand with a need to ensure end-to-end security.

5

Multi Squared: Interoperability for Plug&Charge Solutions

To achieve standardization and interoperability as multiple market players develop Plug&Charge services, collaboration among the various stakeholders is crucial. Through collaboration, the eMobility industry can work towards establishing common standards and protocols, as well as ensuring that different PKIs and ecosystems can work together and in parallel. This not only benefits the industry by enabling more efficient and effective operations, but it also benefits consumers by providing the best possible charging experience across different networks and providers.

We have identified four major opportunities for interoperability throughout 2022: With ISO 15118-20, the International Organisation for Standardisation released the update to ISO 15118-2. As such, considering multi-standard approaches has become vital to the mainstream adoption of Plug&Charge.

Similarly, Multi-Contract Handling has remained a much-conversed topic that enables maximal flexibility for EV drivers, but requires close collaboration between OEM, Plug&Charge operator, and MO.

With several Plug&Charge services about to enter the market, operators and stakeholders must also consider interoperability between ecosystems. In the same breath, we must also consider the integration of multiple V2G roots into a single Plug&Charge ecosystem. All these opportunities for interoperability must be realised to ensure an open and fair market to all actors, and they require the collaboration of major industry stakeholders.

Such multilateral collaboration can take many forms, such as industry associations like CharIN, working groups such as the Plug&Charge Protocol governance group, and open forums at industry events. These platforms provide a space for stakeholders to share ideas, discuss challenges, and develop solutions collaboratively. They also enable stakeholders to coordinate their efforts.

5.1 Multi-Standard Interoperability

To ensure seamless communication between electric vehicles and charging stations, it is crucial for the Plug&Charge ecosystem to be fully equipped to handle ISO 15118-2 and ISO 15118-20.

- ISO 15118-2 is the current global standard that governs the direct communication between the electric vehicle and the charging station. It specifies the communication protocol, which includes elements such as authentication, billing, and authorization.
- ISO 15118-20 is the newer, follow-up standard to ISO 15118-2. It is expected to be implemented in the market in the coming years. It is designed to provide an extended set of features, such as more advanced communication security, and bidirectional power transfer capabilities, which can be used for vehicle-to-grid (V2G) use cases.

These two norms will run parallel to each other for a few years, and it is imperative that every EV and EVSE (electric vehicle supply equipment) be ready to communicate through both protocols to allow for the best possible interoperability.

At present, Hubject's solutions based on ISO15118-2 are being globally rolled out. Solutions based solely on the new ISO15118-20 norm will be implemented in the market over the next few years. For the interim period of transition, it is essential for the Plug&Charge ecosystem to be able to provide Plug&Charge data creation and flow for both norms at the same time to ensure interoperability.

Should ecosystem participants hesitate to commit to the use of both norms, there may be issues with compatibility and communication between EVs and charging stations. This would have consequences for the EV driver experience: longer wait times for charging, decreased efficiency, and increased frustration. Therefore, it is imperative for all Plug&Charge stakeholders to be fully prepared and able to handle both ISO15118-2 and -20 for the foreseeable future.

5.2 Multi-contract Handling

The Plug&Charge ecosystem must be capable of accommodating multiple contracts for a single EV to ensure the best possible EV driver experience. Fortunately, Hubject's Open Plug&Charge Protocol are equipped to handle this functionality.

The Plug&Charge ecosystem already permits the use of multiple contracts for a single EV, which is crucial to offer end-customers the freedom to choose their preferred MO. Multi-Contract Handling can be achieved through telematic installations or the EVSE (Electric Vehicle Supply Equipment).

Hubject offers this service as part of its Plug&Charge solution. The ability to have multiple contracts in a single EV is important, and it is already possible under ISO 15118-2. The new ISO15118-20 standard provides an additional feature that allows native installation of multiple contracts via the EVSE.

For further insights, please refer to the whitepaper:
https://info.hubject.com/vw_multicontract

5.3 Multi-Ecosystem Connections

Hubject is committed to multilateral collaboration with eMobility industry players, as this an important step towards achieving standardization and interoperability in the Plug&Charge ecosystem. This effort is crucial to provide high-quality services for both industry players and end-consumers.

As various Plug&Charge solutions prepare to enter the market, it is essential that there is interoperability between emerging ecosystems. Industry players who have already committed to the existing Plug&Charge ecosystem will benefit from access to multiple solutions with minimal exertion, which serves to ensure a seamless charging experience for the EV drivers.

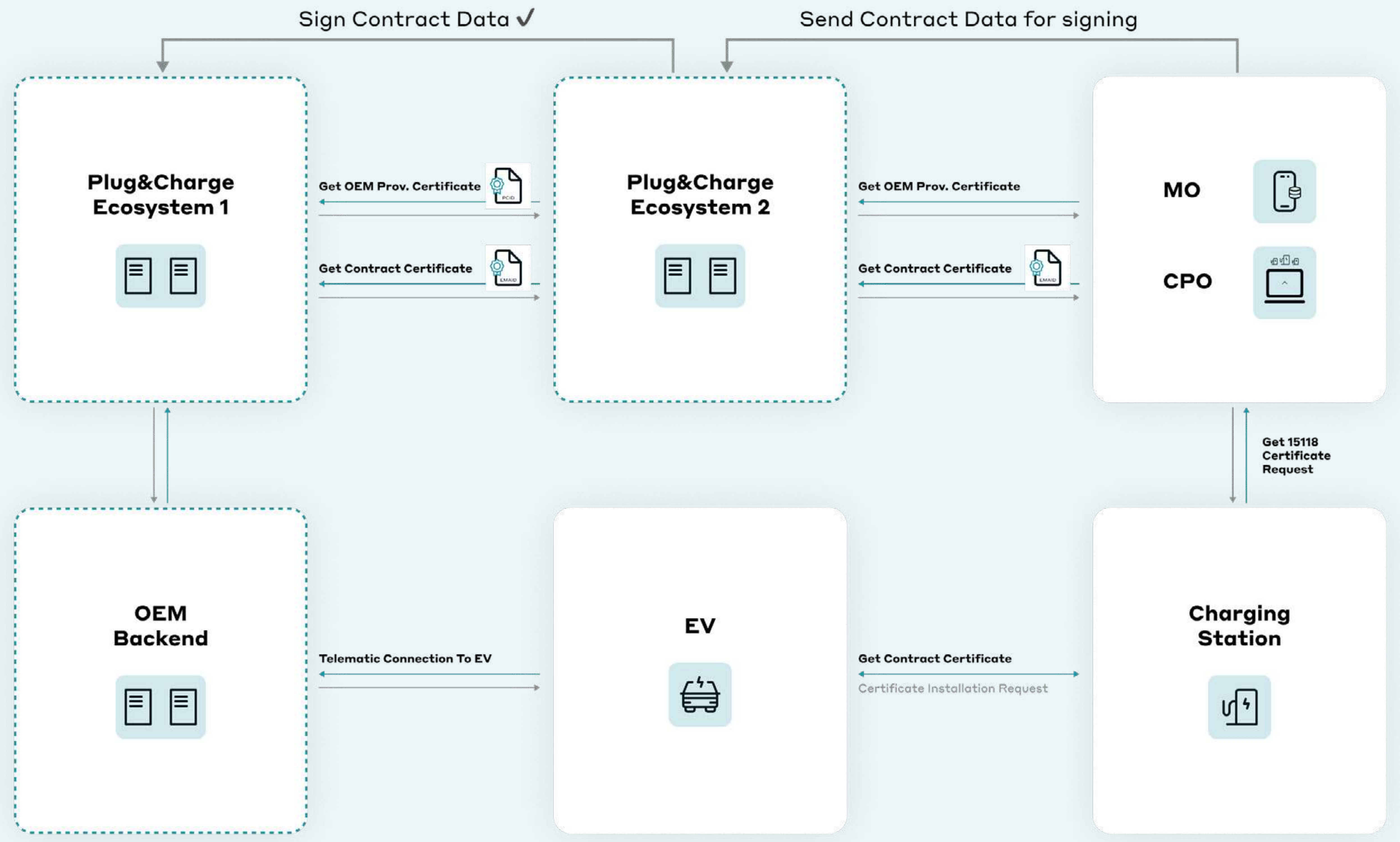
Like the current use case of eRoaming for public EV charging, consumers will soon expect to be able to use the Plug&Charge solution of their electric vehicle at any Plug&Charge capable charging station, regardless of which ecosystem it may be connected to. Hubject believes that it is the responsibility of the eMobility ecosystem to provide this experience in order to accelerate EV mass adoption.

While there is no plurality of solutions based on ISO 15118-2 as of today, Hubject is supporting the growth of diverse Plug&Charge technology by establishing interoperability in research projects and test cases. In November 2022, leading players in eMobility joined together to demonstrate technical interoperability between Plug&Charge ecosystems, showcasing the culmination of a research project that began in 2021.

The project involved the knowledge and innovation center from the Netherlands, ElaadNL, the French research foundation Vedecom, and Hubject. The showcase provided detailed technical insight into how Plug&Charge ecosystems can intersect to provide a seamless experience for the EV driver.[15]

The research findings show that ecosystem interoperability requires a joint protocol to succeed. Communication protocols play a vital role in ensuring the interoperability and seamless functioning within the electric vehicle (EV) charging ecosystem. During the showcase, Hubject's Open Plug&Charge Protocol (OPCP)[16] was used.

For the exchange of certificates, the research project implementation opted for a "pull/push by request" solution: If requested data, such as a provisioning certificate by an MO is not found in ecosystem A, the system would then forward the request as a broadcast to another Plug&Charge ecosystem until the dataset is found. This roaming-type process benefits all ecosystem participants who have already implemented one Plug&Charge solution and are connected to a Plug&Charge ecosystem, as they do not need to integrate with other ecosystems.



[15] To view the showcase, click: https://www.youtube.com/watch?v=2eAyB4X5BiM

[16] For more Information on the OPCP, please see the appendix.

5.4 Multi-V2G Root

The idea of having two productive Plug&Charge ecosystems in the eMobility industry is unlikely to become a reality soon. However, it is realistic to expect the development of multiple V2G-Public Key Infrastructures (V2G-PKI). In traditional IT Security systems, having multiple PKIs is a common practice that diversifies the trusted Certificate Authorities pool and minimizes the risk of tampering. Given the players involved in the Plug&Charge ecosystem, it makes sense for some to develop their own PKI to be used by partners within the ecosystem. Nevertheless, a standalone V2G-PKI is not useful. The certificates of a PKI need to be issued, stored, and used by a Plug&Charge Ecosystem based on the VDE Application Guide. For example - CharIN is currently creating a PKI to be integrated into Hubject's Plug&Charge ecosystem.

The problem the industry is currently facing is that the current standard, ISO 15118-2, that is the basis of implementation by most stakeholders, was developed under the assumption that there will be a single PKI with a single V2G root CA serving as the trust anchor. ISO 15118-2 does not define a process of cross-certification for multiple PKIs, which adds complexity to an already complex ecosystem. Any cross-certification in ISO 15118-2 will be proprietary any will most likely not be adopted by the market.

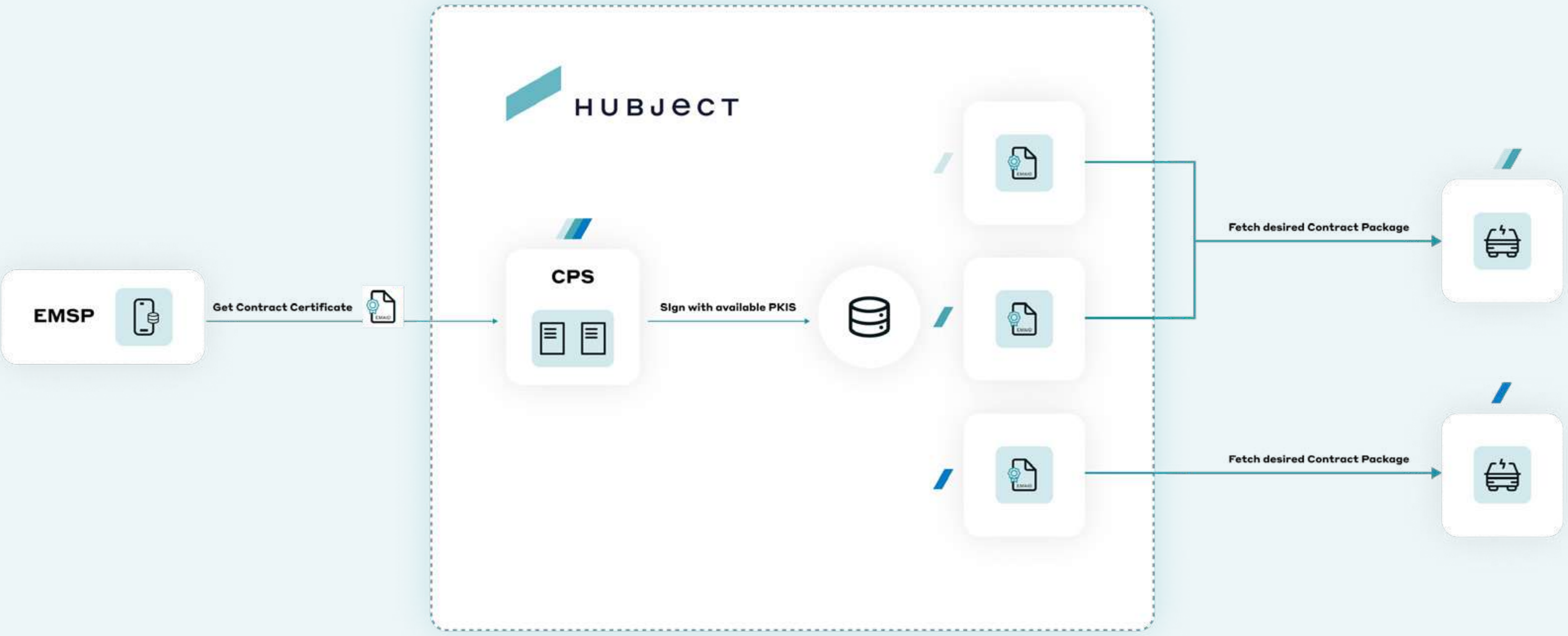
As of 2022, every partner using Hubject's ecosystem is using a single V2G Root Certificate Authority to create relevant certificates, meaning that all players agree to use this PKI as their trust anchor for successful authentication. The Multi-V2G-PKI use case is yet largely theoretical. But once a second PKI is operational, it is quite possible that the EV OEM and the CPO will use PKI that cannot cross-sign certificates, and authentication between the two will fail.

To resolve this issue using the ISO 15118-2 standard requires enabling the signing of contract certificate with multiple V2G-PKIs in the Hubject ecosystem.
EV manufacturers will have to sacrifice storage space in the vehicle's a memory respectively to save multiple V2G Root certificates from multiple CAs.

To gather the different V2G-Roots, the V2G root certificate from the second PKI can be saved to Hubject's Root Certificate Pool, creating a unified information source. Alternatively, a certificate trust list is discussed also on EU-Level.

In the concept of Multi V2G-Root Ecosystems, the EV manufacturers can select the required signed contract bundle from the contract certificate pool and install it into the EV.

MO/EMP solution for the Multi V2G Roots case



The Multi-V2G-PKI use case will likely resolve itself once ISO 15118-20 becomes the primary standard used. ISO 15118-20 provides guidelines for implementing multiple PKI in one ecosystem and explicitly defines the process for cross-certification. However, the switch from the current standard to ISO 15118-20 is not expected anytime soon.

Additionally, cross-certification is quite complicated on a governance level. It remains to be seen how this will be adopted by the market.

Key takeaways

Stakeholders looking to integrate Plug&Charge services into their offerings should consider how the Plug&Charge operators are approaching questions of interoperability on all levels: From enabling the use of both ISO standards in parallel, to offering Multi-Contract Handling, to the interoperability with other solutions set to enter the market, be that another ecosystem, or a non-proprietary V2G root.

Multi-ecosystem and multi-V2G-PKI use cases have shown that ecosystem interoperability requires an open collaboration between eMobility industry stakeholders. The transition from ISO 15118-2 to -20 is expected to take several years. As the Plug&Charge ecosystem is reaching mainstream adoption, this requires all stakeholders to prepare to support both norms in parallel for some time.

For the time being, Stakeholders must prepare for the integration of the Multi-V2G use case. CPOs and OEMs need to be able to integrate multiple V2G Roots into their systems. If they cannot, they should choose a V2G root that is widely used to ensure EV drivers receive the best possible access.

Plug&Charge or V2G root operators that are new the market should prove willingness to create and participate in fully interoperable ecosystems by, for example, using a joint communication protocol. Differentiation between Plug&Charge operators and Plug&Charge solutions will naturally occur based on their varying business models.

Ultimately, the promise of shared standards and protocols encourages more eMobility players to invest in the implementation and rollout of Plug&Charge solutions which will benefit all stakeholders, provide a seamless charging experience for EV drivers and accelerate EV adoption.

Further Reading

HUBJECT

IN PARTNERSHIP WITH

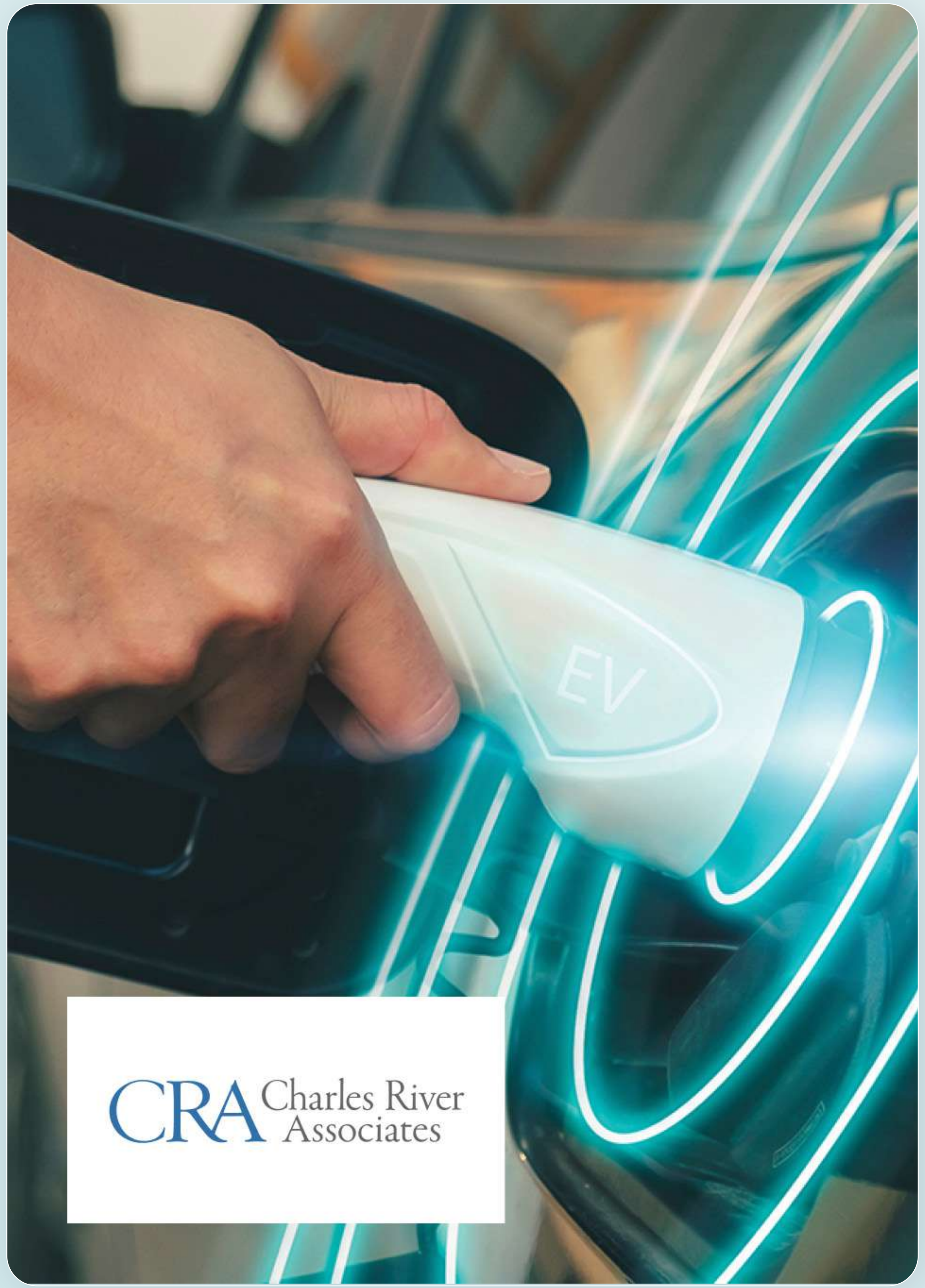
Plug&Charge Multi-Contract Handling

Handling of multiple contracts with Plug&Charge based on ISO 15118-2 and -20

Plug&Charge
is now!

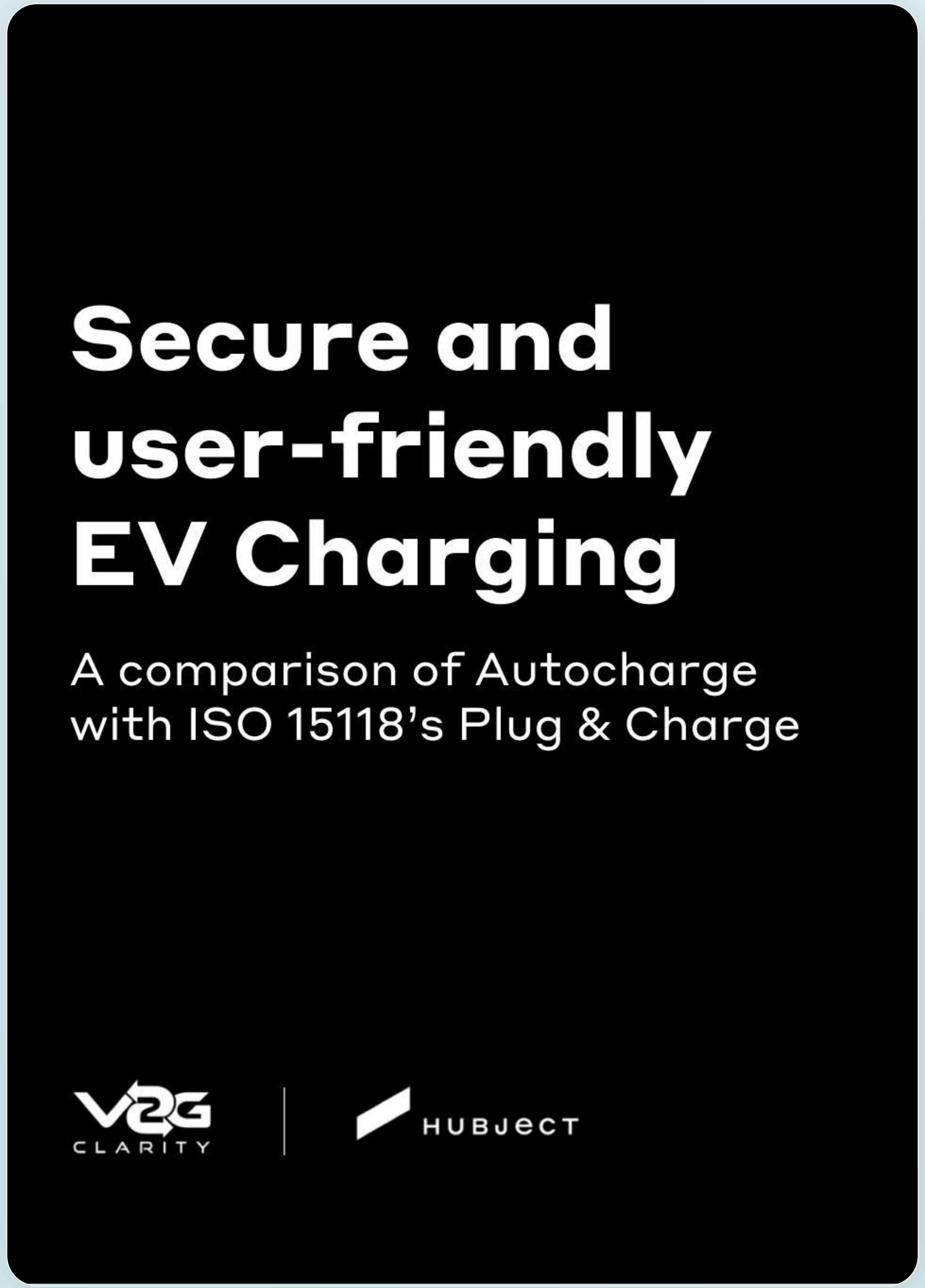
Plug&Charge Multi-Contract Handling

Read now



Introduction to V2G

Read now



Secure and user-friendly EV Charging

A comparison of Autocharge with ISO 15118's Plug & Charge

Secure and user-friendly EV Charging

Read now

Public Key Infrastructure

EXPLORING THE

PUBLIC KEY INFRASTRUCTURE

FOR

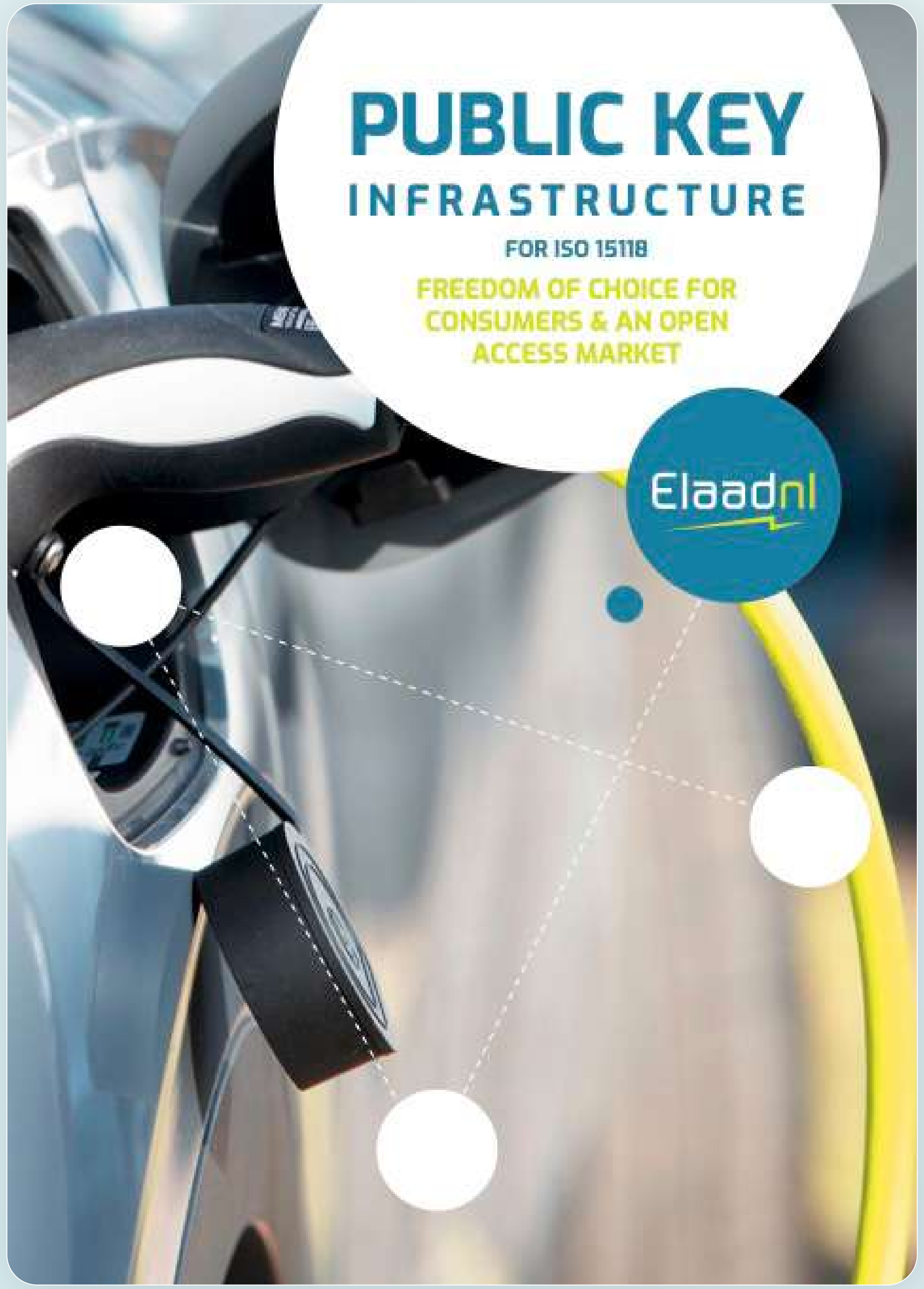
ISO 15118

IN THE

EV CHARGING ECOSYSTEM

Elaadnl

Read now



PUBLIC KEY

INFRASTRUCTURE

FOR ISO 15118

FREEDOM OF CHOICE FOR CONSUMERS & AN OPEN ACCESS MARKET

Elaadnl

Read now

Appendix

All Plug&Charge enabled EVs in 2022

VW	ID.x Series,	active
Audi	e-tron 50, 55, s	active
Daimler	EQS, EQA	active
Porsche	Taycan	active
Ford	Mach-E, E-Transit	active
MAN Truck & Bus	Lion City E	active
Skoda	Enyaq	active
Seat Cupra	Cupra Born	active
Genesis	GV60, GV70, G80	2023
BMW	iX, I7	2023
Volvo	Tbd	2023
Lucid	Air	2023

Open Plug&Charge Protocol (OPCP)

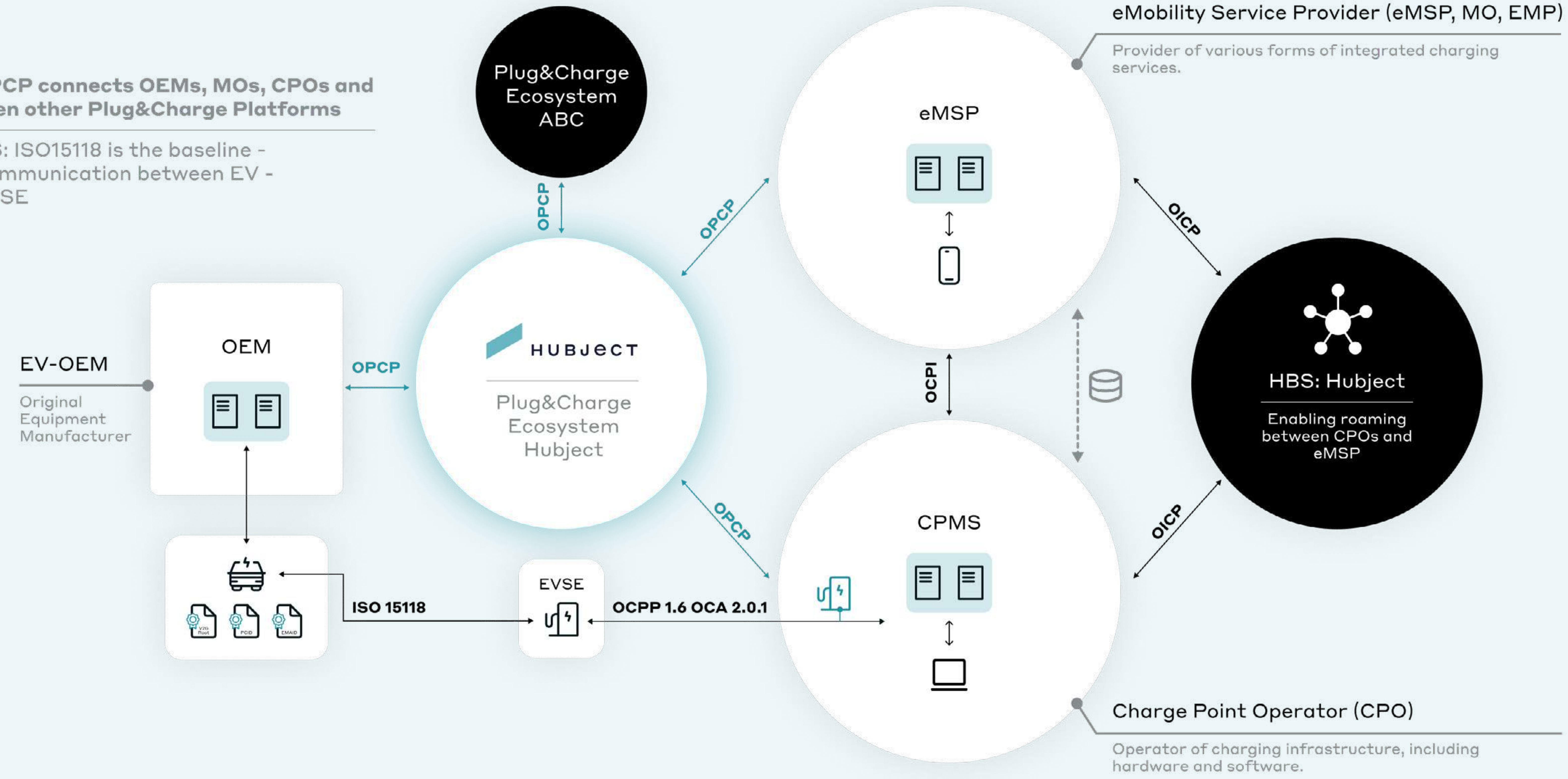
Communication protocols play a vital role in ensuring the interoperability and seamless functioning within the electric vehicle (EV) charging ecosystem.

The primary protocol for Plug&Charge is the eponymous Open Plug&Charge Protocol (OPCP), which was published by Hubject on Github in early 2022.i Based on the ISO 15118-2 and VDE Application guide, OPCP governs the exchange of information between players in Hubject's Plug&Charge ecosystem. It also allows the connection multiple Plug&Charge VDE application guide-based systems.

Hubject's Plug&Charge Protocol has been extensively tested in real-world scenarios and has been in use by market players since 2019 with global players like Porsche, Ionity and Electrify America. As the only productive solution on the market, OPCP has become the standard protocol for the Plug&Charge ecosystem. By using the OPCP as their communication protocol, eMobility players looking to develop their own Plug&Charge solution can ensure interoperability with existing solutions.

The role of the OPCP in the existing Ecosystem

— Plug&Charge Ecosystem


Plug&Charge Ecosystem ABC
OPCP
OEM
EV-OEM
Original Equipment Manufacturer
OPCP
HUBJECT
Plug&Charge Ecosystem Hubject
OPCP
OPCP
eMSP
OCPI
CPMS
OICP
OICP
HBS: Hubject
Enabling roaming between CPOs and eMSP
EVSE
ISO 15118
OCPP 1.6 OCA 2.0.1

OPCP connects OEMs, MOs, CPOs and even other Plug&Charge Platforms

P.S: ISO15118 is the baseline - Communication between EV - EVSE

eMobility Service Provider (eMSP, MO, EMP)

Provider of various forms of integrated charging services.

Charge Point Operator (CPO)

Operator of charging infrastructure, including hardware and software.

Infographic: The Role of the OPCP in the existing ecosystem

Development of a Non-Proprietary Communication Protocol for Plug&Charge Solutions

Hubject has taken the initiative to create a governance group with the goal of developing a fully non-proprietary communication protocol that can be used by all Plug&Charge ecosystems. The collaboration charter, defined in late 2022, outlines the purpose of the initiative. The protocol is currently in its development phase. The objective is to create a joint and neutral Plug&Charge protocol that will be backward compatible with OPCP and enable improvements, new use cases and ideas.

The development of this shared protocol encourages eMobility businesses to invest in developing Plug&Charge solutions based on ISO 15118-2 or ISO 15118-20, resulting in a more diverse market offering while ensuring interoperability. Open collaboration enables the eMobility industry to move towards a more unified and integrated Plug&Charge ecosystem that benefits both consumers and service providers.

Hubject handed over the governance of the Plug&Charge Protocol group to CharIN to facilitate the communication platform for the participating companies.

Open Plug&Charge Test Environment

In November 2021, Hubject established a free testing environment based on ISO15118-2.ii Access to a neutral and free testing environment ensures that stakeholders can experience the functions of Hubject's Plug&Charge ecosystem and test their own solutions with the Hubject V2G-PKI. This requires no commercial agreement with Hubject, as the goal is to catalyse the adoption of Plug&Charge. With the launch of the first available V2G-PKI for the new ISO15118-20 standard in 2022, this test environment has become the system to use for multi-standard interoperability testing.[17]

[17] https://www.hubject.com/blog-posts/hubjects-plug-charge-team-is-first-to-launch-iso15118-20-public-key-infrastructure-in-their-free-testing-environment

HUBJECT