SUSTAINABLE TRANSPORT FORUM

European Commission

# DEVELOPMENT OF A GOVERNANCE AND ARCHITECTURE FRAMEWORK FOR THE IMPLEMENTATION AND OPERATION OF A PUBLIC KEY INFRASTRUCTURE (PKI) ECOSYSTEM FOR E-MOBILITY IN THE EU

**ACTIVITY 2 adopted by the STF Sub-group on Governance & Standards on 7 July 2023**

**LEGAL NOTICE**

This publication is a report by the Sustainable Transport Forum (STF) Sub-group on Governance & Standards, the European Commission´s expert group on alternative fuels infrastructure. It aims to provide evidence-based scientific support and recommendations to the European policymaking process. The document reflects the views only of the members of the STF Sub-group on Governance & Standards. The document does not imply a policy position of the European Commission and the European Commission is not liable for any consequence stemming from the reuse of this publication. More information on the European Union is available on the Internet (http://www.europa.eu).


| | | | |
|---|---|---|---|
| PDF | ISBN 978-92-68-06051-3 | doi:10.2832/010726 | Catalogue number:MI-07-23-280-EN-N |

Luxembourg: Publications Office of the European Union, 2023


**EUROPEAN COMMISSION**


Directorate-General for Mobility and Transport (DG MOVE)
Directorate B — INVESTMENT, INNOVATIVE AND SUSTAINABLE TRANSPORT
Unit B4 — SUSTAINABLE & INTELLIGENT TRANSPORT

*Contact:* Dr. SAKI GERASSIS DAVITE (Chair STF Sub-group on Governance & Standards)

*E-mail:* Saki.GERASSIS-DAVITE@*ec.europa.eu*

*European Commission*
*B-1049 Brussels*





How to cite: European Commission, Directorate-General for Mobility and Transport, Report (Activity 2) of the STF Sub-group on Governance & Standards: *Development of a governance and architecture framework for the implementation and operation of a Public Key Infrastructure (PKI) ecosystem for e-mobility in the EU*, Publications Office, 2023, https://data.europa.eu/doi/10.2832/010726

# Contributors

| DRAFTING CONTRIBUTORS | |
|---|---|
| **ACEA** | Adriana Pop |
| **CHAdeMO** | Uwe Likar |
| **ChargePoint** | Kor Meelker |
| **ChargeUp Europe** | George Niland<br>Wilhelm Henriksson |
| **CharIN** | Michael Keller<br>Glenn Cezanne |
| **DigiCert** | Stephen Davidson |
| **ECOS** | Luka de Bruyckere<br>Tomi Engel |
| **ElaadNL** | Lonneke Driessen-Mutters |
| **EnBW** | Stefan Scheubner |
| **Enel X** | Giovanni Coppola |
| **E.ON** | Kai Toekan |
| **EVRoaming Foundation** | Michel Bayings |
| **Gireve** | Jean-Marc Rives<br>Margaux Vandeville |
| **Hubject** | Christian Hahn |
| **IN Group** | Tamás Horvath |
| **Shell** | Karl Weinreich<br>Sebastian Vetterlein |
| **SmartLab (e-clearing.net)** | Moritz Dickehage |
| **Tesla** | Mattheo van der Molen<br>Koen Schröder |
| **Vedecom** | Roch Elkhoury<br>Mourad Tiguercha |
| **Virta** | Jussi Ahktikari |

| OBSERVERS | |
|---|---|
| **Germany** | Jan Wegener |
| **Greece** | Ilias Pasios |
| **California Energy Commision** | Jeffrey Lu |
| **PwC (Commission Support Study)** | Enrico Gaspari<br>Andrea De Angelis<br>Vivian Leamy |
| **SAE** | Tim Weisenberger |

| EDITION | |
|---|---|
| **European Commission** | Saki Gerassis |

# Table of Contents

# List of Acronyms

| | |
|---|---|
| **AC** | Alternating Current |
| **AFIR** | Alternative Fuels Infrastructure Regulation |
| **BMS** | Battery Management System |
| **CB** | Certificate Bundle |
| **CC** | Cross Certification |
| **CCP** | Contract Certificate Pool |
| **CO** | Contract Owner |
| **CP** | Charging Point & Certificate Policy |
| **CPO** | Charging Point Operator |
| **CProvS** | Certificate Provisioning Service |
| **CR** | Cross Recognition |
| **CTL** | Certificate Trust List |
| **CS** | Charging Station |
| **CSMS** | Charging Station Management System |
| **DC** | Direct Current |
| **DSO** | Distribution System Operator |
| **EMSP** | Electromobility Service Provider |
| **EV** | Electric Vehicle |
| **EVCCID** | Electric vehicle communication controller ID |
| **ISO** | International Standardisation Organization |
| **HMI** | Human Machine Interface |
| **MNA** | Multi Non-regulated Architecture |
| **MRA** | Multi Regulated Architecture |
| **OEM** | Original Equipment Manufacturer |
| **PA** | Policy Authority |
| **PCID** | Provisioning Certificate ID |
| **PKI** | Public Key Infrastructure |
| **PnC** | Plug and Charge |
| **Root CA** | Root Certificate Authority |
| **RCP** | Root Certificate Pool |
| **RSP** | Roaming Service Provider |
| **SoC** | State of Charge |
| **STF** | Sustainable Transport Forum |
| **Sub CA** | Subordinate Certificate Authority |
| **TLM** | Trust List Manager |
| **TLS** | Transport Layer Security |
| **TSO** | Transmission System Operator |

| | |
|---|---|
| **UNA** | Unique Non-regulated Architecture |
| **URA** | Unique Regulated Architecture |
| **V1G** | Smart charging |
| **V2G** | Vehicle-to-Grid |
| **V2H** | Vehicle-to-Home |


# Introduction

SUSTAINABLE TRANSPORT FORUM

# 1. Introduction

Electromobility represents a strategic international market. **The set-up and functioning of a Public Key Infrastructure (PKI) is considered essential to address the future communication and security needs among the different actors in the recharging[1] ecosystem**. When the European Commission launched the discussion of this topic in the Sustainable transport Forum (STF) at the beginning of 2022, it was brought to light that several PKIs would have to co-exist in the European market, responding to the continuous developing nature of the EV charging industry and the ongoing initiatives of several market players. In a situation where multiple, independent and competing PKIs would co-exist, it is unlikely they will be interoperable by default unless all PKI providers mutually agree to 'trust' each other by recognising a series of governance, architecture and operational aspects.

Not addressing PKIs technical interoperability could disrupt the effective functioning of the EV charging ecosystem in the EU, leading to the fragmentation of charging services. This situation would worsen the quality of services offered, thus, frustrating users and impacting the overall acceptance of electromobility.

In a scenario where the owners and participants of multiple PKIs are also business competitors, the lack of clear market rules could create a situation that hampers trust and cooperation. This situation may lead to a market based on a set of independent, non-interoperable PKIs. Overall, this poses important risks for the European electric vehicle ecosystem. On the one side, there exists a possibility of 'user lock-in' where users can only make use of PKI services in recharging stations that are part of the PKI of choice of their vehicle manufacturer and/or electromobility service provider (EMSP). On the other side, it could materialise the development of 'competition lock-out' where potentially leading PKI governing organizations might have the ability to reject certain parties and new entrants from participating in their PKI system.

To avoid this potential scenario, the European Commission aims to facilitate the discussion among industry actors in the context of the STF Sub-group on Governance and Standards, gathering relevant technical information and recommendations in support of potential policy provisions and measures that would underpin a common approach in the EU. **It is also the intention of the European Commission that this work, based on strong public-private dialogue and cooperation, could serve as a reference for other regions** aiming to support the development of PKI services in the electric vehicle charging space.

An **open and interoperable EU PKI ecosystem** that ensures fairness and a level playing field requires a joint effort from the industry. This is a joint effort between OEMs, CPOs, EMSPs, DSOs, TSOs and e-roaming platforms. Agreement of the electric vehicle charging industry on the governance and architecture of the future EU PKI ecosystem is therefore crucial to ensure a competitive electromobility market in the coming years.

[1] Recharging and charging are used indistinctly throughout the document.

# 2. Objective and structure

This document elaborates Activity 2 of the Sustainable Transport Forum (STF) Sub-group on Governance and Standards as reflected in the Working Programmes 2022 and 2023. It plays an important role in the information and consideration by the European Commission on the possible provisions and standards that could be prescribed in future secondary legislation under the Alternative Fuels Infrastructure Regulation (AFIR).

The **objective** of this document is to gather the recommendations from the members of STF Sub-group on Governance and Standards to the Commission on the preferred option for a future governance and architecture framework of the EU PKI ecosystem, based on the standard ISO 15118 (vehicle-to-grid communication interface), and considering other additional technical aspects required.

**The European Commission is aimed at supporting members of the STF to develop and implement a PKI governance and architecture in the EU** by complementing key standards identified[2] (i.e., ISO 15118) in order to achieve a seamless and fully interoperable EV recharging ecosystem. This activity is necessary because it did not exist a market consensus on how PKI systems would intereact among themselves, and further, how a future EU PKI ecosystem[3] would be governed and operated in the EU, ensuring an open an competitive market that meets user needs.

In this context, the way forward is conceived to be based on strong public-private cooperation, namely collective dialogue and work by industry in cooperation with the legislator at a European scale and not on the work of individual actors alone developing specific solutions attending to exclusive business and/or national interests. The objective is to lay down the basis for a future open and competitive market, removing the risk of vendor lock-in or an increased complexity for a nascent PKI ecosystem that could affect the proper implementation of crucial standards such as ISO 15118.

Based on the context elaborated above, a number of stakeholders called the European Commission indicating that **the involvement of the regulator could help to structure the discussion and develop a common European approach** that could be supported by the relevant legislation, i.e. AFIR. The depth of Commission involvement in the context of this activity under the STF is limited to support the definition of a single approach that reflects the preferred governance and architecture option based on the proposed alternative raised by the members of the sub-group attending to industry projects under development at the moment of developing this document. Members of the sub-group have contributed to detail the technical characteristics of each option, finding an optimum solution with the moderation support of the European Commission.

To carry out this main objective, the discussion has been structured in three parts that are reflected in this document in three blocks. The intention is to develop a comprehensive overview around the need and purpose of a PKI ecosystem for electromobility (Block 1), explaining, from a high-level perspective, what will be the main governance and

[2] European Commission, Directorate-General for Mobility and Transport, *Mapping of the discussion concerning standards and protocols for communication exchange in the electromobility ecosystem*, Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2832/6763

[3] Independently if it consists of one or multiple PKI(s)

architecture approach to be followed in the European Union (Block 2). Finally, the document identifies from the viewpoint of industry members those regulatory needs and other important outstanding technical aspects (Block 3) that need to be addressed. More precisely, the concrete objectives of the document for each section are to:

**Block 1: A Public Key Infrastructure (PKI) for e-mobility**

- Present and elaborate the added value of an electric vehicle charging PKI ecosystem and their specific features, such as Plug and Change (PnC), from a user perspective.
- Reflect the impact on payment options, including e-roaming, smart and bidirectional charging, dynamic tariffs, price transparency and infrastructure quality.
- Identify key existing PKI projects and services at the moment of performing this analysis.
- Provide a general summary of the possible governance and architecture options for the functioning an operation of an EU PKI ecosystem for e-mobility.

**Block 2: Identification of a high-level governance and architecture framework for the functioning and operation of a EU PKI ecosystem in the European Union**

- Gather recommendations on the preferred PKI governance and architecture solution that duly considers the needs of the different market players and feature quantifiable arguments, why to be chosen.
- Conclude a preferred governance and architecture framework for the set-up and operation of an open and competitive PKI ecosystem in the EU.
- Describe the ongoing individual implementation by market actors and lays down the foundations for the implementation of the proposed PKI governance and system architecture.

**Block 3: Identification of regulatory needs and other outstanding technical aspects**

- Conclude on vehicle and infrastructure hardware readiness, standard(s) and compliance dates in relation to communication exchange and PKI functioning, building on the conclusions and recommendations of Activity 1.
- Determine the exact role of the standard ISO 15118, and its different parts, as the preferred EU option for the communication between the EV and the charging point (CP) as part of a PKI governance framework. Likewise, the role and function of other protocols and/or standards supporting the PKI system shall be identified.
- Identify and describe relevant gap and limitations that could preclude an open and fair e-mobility ecosystem.
- Identify specific regulatory (policy) needs in support of the preferred governance and PKI architecture model.
- Recommend concrete policy and technical actions, considering both vehicle and infrastructure needs, for the relevant legal instrument(s) (e.g., AFIR, vehicle type approval, etc.).

Importantly, this document ***Recommendations on the development of a governance and architecture framework for the implementation and operation of a PKI ecosystem in the European Union*** has been developed in synergy with the ***Commission Support Study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118.***

Based on the high-level governance and architecture framework for the EU PKI ecosystem proposed in Block 2 of this document, the European Commission invited members of the STF Sub-group on Governance and Standards to take active part in Phase 2[4] of the ***Commission Support Study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118*** in order to elaborate the relevant policy, technical and governance elements required to implement and support that framework via legislation and the corresponding market rules. As a result, both documents (i.e., STF recommendations and the Support Study) aim to provide clear evidence to the European Commission on how to proceed on this matter. The relevant materials of the Commission Support Study are published in a separate publication report.

[4] From January-June 2023


# Block 1: A Public Key Infrastructure (PKI) for e-mobility

SUSTAINABLE TRANSPORT FORUM

# 1. What is a PKI for e-mobility and what is the added value for the end user?

A **Public Key Infrastructure (PKI)** is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption[5].

A PKI is considered of major importance in the electric vehicle charging ecosystem as it has the potential to address the needs of EVs, charging point operators (CPOs) and electromobility service providers (EMSPs), facilitating the offering of new services (e.g., PnC) to the user by providing trust. From user authentication to data protection, a PKI can also help secure and speed-up the EV charging process.

More generally, for electromobility a PKI can be understood as a wide trust-based platform to digitally authenticate users, EVs, charging stations and EMSPs, but also facilitating the participation and offering of services by e-roaming platforms and energy grid operators. It can encrypt and authenticate data transfers such as vehicle-to-charging point (EV-CP), vehicle-to-service provider (EV-EMSP) and charging station-to-charging station (CS-CS), offering security across platforms.

In that context, members of the STF Sub-group on Governance and Standards start from the firm premise that a PKI shall be considered as the central part of the cybersecurity basis for electro-mobility. Importantly, the set-up and operation of a PKI will not come automatically. Manifold elements are needed like adequate governance rules and data exchange mechanisms that are intrinsic to the PKI, but subject to concrete principles agreement by members of the ecosystem. These additional elements required to put in place a fully operational PKI system could be covered by the term **"extended PKI"**.

## 1.1. Expected roles and functions of a PKI and benefit to the end user

The main function of a PKI is to be a trusted anchor between different actors. The PKI enables participating actors to establish secure automatic communications between their systems, to authenticate specific data elements, ensuring data integrity.

For the **EV end user**, the PKI operations (e.g., authentication, billing) should be secured and transparent. In practice, the PKI would be technically imperceptible for the eyes of the user, who will see the benefits in terms of the services offered. Moreover, the PKI brings a quality leap in terms of security. The end user is protected from potential identity management without authorisation (including identity usurpation), transactional data disclosure and overall manipulation when using EMSPs. This enhanced level of security has a great impact, for example, when it comes to the fulfilment of service access control and billing.

In this context, a secure authentication process means that at any time each actor is clearly identified and authenticated beforehand, and all other actors may clearly trust (or not) and

[5] See ISO/IEC 27099:2022 Information technology - Public key infrastructure - Practices and policy framework https://www.iso.org/standard/56590.html

interact with it. Further, a secure data-transfer means that the source and the destination of any data transfer are clearly identified and authenticated, and that the flow is not "readable" by any other actor (encryption).

For the different actors of the **EV charging ecosystem** (OEMs, CPOs, EMSPs, e-roaming platforms, DSOs, TSOs), the PKI can be used to secure the manifold existing communications lines (e.g., EVSE-CSMS, EV-EVSE, EV-BMS, etc.), fully automate contract-based charging (PnC), communicate EMSP recharging tariffs, exchange energy metering data and support the development of future applications and services. At the moment of developing this document, there is a clear consensus and market ambition around the use case of a PKI to support the implementation and offering of PnC services. In the future, other use cases could be also added to a established PKI ecosystem, depending on its maturity and market interest.

It must not be forgotten the risks that could be mitigated and avoided by the deployment and operation of a wide PKI for e-mobility in the EU, based also on clear rules for potential participants from other non-EU regions. For example, a PKI for EV charging would reduce the risk of potential user identity management without authorisatoin, payment fraud, recharging unavailability. In addition, a PKI will also mitigate risks for other ecosystem actors such as e-roaming platforms and grid operators. The PKI for e-mobility, within a proper ecosystem, is therefore understood as a must from OEMs to electricity networks protection and communication with the recharging ecosystem.

From an **application perspective**, a PKI provides secure authentication and authorization. Digital certificates in accordance with the standard ISO 15118 are the instrument used to secure the communication between EVs and charging stations. With that technical basis, for example the standard ISO 15118 enables the PnC feature.

> While the technical framework for a PKI is introduced in the ISO 15118 standard, additional **governance, technical and regulatory measures** are needed to ensure interoperability, user free of choice and a level playing field for participant market actors.

For the technical solutions to work together there needs to be a standard way to implement the digital secure communication. More broadly, a **PKI ecosystem** needs to be based on a governance and architecture that allows for interoperability with other **PKI systems**. Further, for different market actors to trust multiple PKI systems, there needs to be a series of quality and operational rules, such as those gathered in the so-called Certificate Policy (CP) and in other relevant audit and assurance requirements. The next section will focus on these aspects.

# 2. Definitions

## 2.1. PKI ecosystem and PKI system

The use of commonly agreed definitions it is of critical importance to ensure technical coherence and homogenous level of interpretability among the actors addressing the governance, architecture and operation of the PKI ecosystem in the EU. At the moment of initiating this discussion, industry stakeholders had different interpretations of the same concept. Consequently, this section aims to reflect a common understanding of the underlying PKI technology based on concise definitions jointly elaborated with members of the STF Sub-group of those key concepts applied to this topic.

First of all, in the context of e-mobility, **a PKI ecosystem is understood and defined as a series of individual PKI systems** – each having its own Root Certificate Authority (RCA), Policy Authority (PA) as well as Certificate and Security Policy (CP and SP) – complying to a common governance and market rules provided by a central authority (i.e., the European Commission). The central authority, which must be neutral and accepted by all market parties, is responsible for setting policies and rules in order for the candidate PKI systems to be included in the ecosystem generated with the relevant technical interoperability solution, such a Certificate Trust List (CTL) approach, thus with the purpose of achieving interoperability inside the PKI ecosystem.

In this context, the PKI ecosystem is accessible by external actors, using services and APIs. These services are operated by services providers and cover generic PKI services (certificates issuing, revocation, etc.) and e-mobility specific services like pools management.

## 2.2. Specific definitions

**Certificate (C)**: A digital file that conforms to the ITU-T Recommendation X.509 and that:

1) identifies the subscriber of the certificate.
2) identifies the authority that issued the certificate.
3) contains the subscriber's public key.
4) provides a validity period for the certificate.
5) is digitally signed by the CA that issues the certificate to provide assurance of the integrity of data contained within the certificate and the identity of the CA that issued the certificate.

**Certificate Policy (CP)**: A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. In general, a CP describes what level of assurance may be placed in certificates that are issued under the policy. More specifically, a CP is an administrative policy that addresses all aspects associated with the generation, production, distribution, accounting, compromise, recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

**Certification practice statement (CPS)**: The certification practice statement describes the necessary and sufficient procedures and controls employed by the CA in issuing, managing, revoking, and renewing or re-keying certificates. The purpose of the certification

practice statement is to clearly define the CA's procedures and practices to manage the risks associated with certificate policies. A useful approach in completing the certification practice statement is to follow IETF RFC 3647 and clearly define the step-by-step practices from certificate request/issuance, certificate verification and required supporting functions. See ISO/IEC 27099:20226.

**Certificate Provisioning Service (CProvS)**: The CProvS provides the interface(s) for the signing process of the contract data set. During the signing process, the relevant contract data (among which the contract-certificate) is collected, prepared, and grouped in a "bundle". This "bundle" is then signed and made available. Note that the "provisioning-Certificate" is required for this process, even if it is not part of the "bundle".

**Certificate Trust List (CTL)**: The CTL is a list of all trusted Root Certification Authorities (Root CAs) in the e-mobility PKI ecosystem. In the EU, the CTL would ensure EU-wide interoperability, trust and security of e-mobility services (i.e., PnC).

**Charge Point Operator (CPO)**: It is the entity responsible for the management and operation of charging stations. Its main responsibilities concern the management of the charging points by means of an IT system, including the billing and invoicing, either directly to the driver or via an e-mobility service provider (EMSP).

**Charging Station – Original Equipment Manufacturer (CS-OEM)**: CS-OEM stands for 'charging station - original equipment manufacturer' and, in the context of electric mobility, is associated with charging station manufacturers.

**Contract Certificate (CC)**: Certificate representing a contract between a mobility operator and one of its customers for the delivery of energy via a charge point.

**Contract Certificate Pool (CCP)**: It is a data exchange and communication facility, on which the asynchronous (and synchronous) exchanges of Contract Certificates (wrapped up in a data set called "bundle") between actors (eMSP, OEM, CPO) are based.

**Certificate Bundle (CB)**: Bundle of data containing mainly the Contract Certificate (CC) used to ensure integrity and authenticity. The Certificate Bundle (CB) when signed by the Certificate Practice Statement (CPS) is called Sign-Certificate-Bundle.

**Contract Owner (CO)**: It is the person in possession of a valid "Plug & Charge" eMSP contract.

**Electric Vehicle - Original Equipment Manufacturer (EV-OEM)**: EV-OEM stands for 'electric vehicle - original equipment manufacturer' and, in the context of electric mobility, is associated with electric vehicle manufacturers. EV-OEMs shall enable an EV drivers to conduct automated charging.

**Electric Vehicle (EV)**: EV stands for a vehicle with electric propulsion with ISO 15118 enablement and a Plug & Charge feature available.

---

[6] See ISO/IEC 27099:2022 Information technology - Public key infrastructure - Practices and policy framework

https://www.iso.org/standard/56590.html

**Electric vehicle communication controller ID (EVCCID)**: It specifies the EV communication controller unique identifier, which is in an embedded IT system within the vehicle, that implements the communication between the vehicle and the charging station in order to support ISO 15118 communication.

**Electric Vehicle Driver (EV Driver)**: EV driver as main user of a charging service and direct beneficiary of any PnC service after activation. The EV driver is able to: 1) Activate or deactivate PnC and 2) Manage PnC contract preferences by means of vehicle userinterface (i.e. app or in-vehicle display).

**E-mobility Service Provider (EMSP)**[7]: Also called "mobility operator" (MO) it means a legal person who provides services in return for remuneration to an end user, including the sale of a charging service. An eMSP offers charging related services to the EV driver such as the location and availability of a charging station as well as to authenticate and pay for a charging session. The EMSP concludes a commercial contract with the EV owner or driver, including the billing process.

**PKI participant**: Entity which makes use of a PKI system, i.e. CPO, EV-OEM or EMSP. The PKI participants are connected via a Sub CA to the Root CA of the PKI system.

**PKI provider**: The general administrator of the PKI and provider of the Root CA. The provider operates the interactions with the PKI participants and associated Sub CAs in addition to the Root CA.

**Provisioning Certificate Identifier (PCID)**: It identifies the EV-OEM provisioning certificate. It is used to ensure a secure way of provisioning the EV with the contract certificate that will be used to support the PnC feature.

**Provisioning Certificate Pool (PCP)**: It provides the interface(s) to exchange the EV-OEM provisioning certificates between EV-OEMs and eMSPs. After the production of the EV, the EV-OEMs can make available the vehicle certificates (OEM provisioning certificates) of EVs in the PCP. The OEM provisioning certificates are used by the mobility operators to create Certificate Bundles (CB). The EMSPs can access to the OEM provisioning certificates by sending the OEM provisioning certificate ID (PCID) of the vehicle certificate, which is issued by the EV-OEM. The PCP delivers the appropriate EV-OEM provisioning certificate and the corresponding Sub-CA certificate chain.

**Roaming Service Provider (RSP)**: It offers roaming services, meaning the exchange of data and payments between CPOs and eMSPs from which an end user purchases a charging service.

**Root Certificate Pool (RCP)**: The RCP is used for the exchange of the Root certificates between the various Root CAs of participants within the e-mobility PKI ecosystem. Each participant can retrieve the Root CAs of the other participants to validate the certificate chains. For Root CAs included in the CTL, the latter is the authoritative source. For any other Root CA, the RCPs are independent.

[7] Or simply referred to as 'mobility operator' (MO)

**Root Certificate Authority (Root CAs)**: The Root Certificate Authority is defined as the entity (or all entities) authorised to issue and self-sign its Public Key Root certificate (trust anchor) within a given PKI system. Root CAs issue certificates to Sub-CAs.

**Subordinate Certificate Authority (Sub-CA)**: A Certification Authority that is issued a CA certificate authorizing it in a PKI hierarchy from a Superior CA.

**V2G Root Certificate Authority (V2G Root CA)**: It is the concrete Root Certificate Authority for Plug and Charge services authorised to issue Public Key Root certificates within the e-Mobility PKI.

The V2G Root CA is the Root CA for SECC (EVSE) certificates and for CPS signature.

The V2G Root CA and all actors that receive certificates from it and use them are subject to the same governance rules of the e-mobility PKI ecosystem. Multiple authorities can co-exist and be set up, for example by OEMs, EMSPs, e-roaming platforms, CSOs, DSOs, etc. Plug and Charge requires a specific V2G Root CA, also referred to as V2G RCA. One or several V2G RCA may be deployed simultaneously in a PKI ecosystem. The V2G Root CA publishes its certificate and registers Sub-CAs that are authorized to produce the needed certificates to operate the services, namely produce leaf certificates for EVSEs.

**V2G Root Operator (V2G Root Operator)**: The V2G Root Operator is responsible for the management of the V2G Root CA, which is the highest trust anchor in ISO 15118. It securely creates a V2G Root certificate that provides for all the stakeholders of ISO 15118. A V2G Root Operator is responsible to deliver Sub-CAs certificates to other operators responsible of delivering EVSE Leaf Certificates, Certificate Provisioning Service (CPS) Leaf certificates and optionally Contract certificates and EV provisioning certificates. A V2G Root Operator may aggregate all or part of these roles in addition to other operators.

**Vehicle1Grid (V1G)**: It means the control of time and magnitude of charging power from a power source to the EV.

**Vehicle2Grid (V2G)**: It means the control of time, magnitude and direction of (dis)charging power from the electricity grid to the EV and back to the electricity grid (grid compliance required)

**Vehicle2Home (V2H)**: It means the control of time, magnitude and direction of (dis)charging power from a home power source to the EV and back to a home power source.

**WMI format**: It consists of a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notification.

## 2.3. The relation between PKI, e-roaming and standards

**A PKI in the EV charging ecosystem is broadly understood by industry stakeholders as a fundamental element for automating and securing the scale-up of e-roaming**. The future possibility of offering to the user contract-based solutions that cover lager recharging networks in a secured and automated manner will depend on the widescale implementation of an efficient PKI system.

E-roaming is expected to enlarge the scope of data exchange to take into consideration new services (e.g., PnC). It is understood that e-roaming platform operators of e-mobility services are not required to have a direct connection with the PKI. Nevertheless, e-roaming operators can take actions to ease the exchange of cyber credentials necessary to produce, transport and distribute certain information elements to the intended users, such as sign charging receipts, sign tariff information or sign meter readings.

Importantly, considering that multiple market actors with different business approaches and services are expected co-exist, **interoperability supported by market rules applicable to involved market actors must be ensured as a foundational capacity** required to guarantee the adoption of e-mobility PKI in all application areas.

In the electromobility ecosystem, **PKI** and **ISO 15118** are often intertwined. Industry members of the STF Sub-group on Governance and Standards deem necessary to clarify that a PKI is not necessarily linked to a single standard.

A PKI plays a vital role in the communication and data transfer for a wide range of processes. In the case of electromobility, the PKI is expected to cover different use-cases as reflected in this document. In this context, ISO 15118 is considered the flagship standard for EV-CP communication, which needs a PKI to enable the use of certificates for securing features like identification and automatic authentication of the driver to authorize the EV charging and the subsequent initiation of the charging process.

Some industry members believe that a PKI system for EV charging should not include just a series of features (e.g., Inter-network e-roaming or automated payment for services) but be open, extensible and scalable to add future use cases. In consequence, these industry members[8] have expressed that a future PKI platform should be "protocol-neutral", meaning that it should not be tied to a concreate feature or use-case (e.g., Plug and Charge) or any other charging protocol.

On that basis, the manner in which the PKI ecosystem with ISO 15118 and additional standards covering new potential needs will be shaped, it will determine the success and competitiveness of the European EV charging industry. ISO 15118 and relevant new standards shall be accessible for everyone. This is understood as a requisite to keep this technology inclusive and open for the entire ecosystem.

[8] ChargeUp and the members of the SAE PKI project

The term **protocol-neutral** captures the sentiment by some industry members about the possible risk of vendor lock-in associated to an improper use of the standard ISO 15118 as part of the PKI governance and archietcture system.

Members of the STF Sub-group on Governance and Standards agree that the future PKI governance and architecture will inherently depend on a series of standards, beyond ISO 15118 for EV-CP communication, which will need to evolve with the time in order to also reflect new use-cases that may appear where the PKI might be also needed.

Therefore, in addition to the role of ISO 15118, the future PKI governance and architecture will need to be able to couple other standards and protocols needed (e.g., CPO back-end, e-roaming, grid services) to ensure the adequate functioning of the EV charging ecosystem. In essence, the future PKI governance and architecture to succeed shall be prepared to adapt and transition to new features and uses cases demanded by the user.

## 2.4. The PKI and the impact on smart and bidirectional charging, dynamic tariffs, price transparency and overall infrastructure quality

For utilities, an open and interoperable PKI system is important too. Utilities operate critical infrastructure and the integration of electric vehicles into the grid constitutes a major challenge that needs to be tackled in a secure manner.

When recharging is coupled to grid-related services, such as smart and bidirectional charging, it becomes critical the safety and security of the process, both from an electrical grid as well as charging perspective. In these situations, members of the sub-group believe that involved systems should be identified and authenticated by means of a PKI before setting up any communication in order to lower the risks of potential attacks or misusages.

With the new version of ISO 15118, i.e. ISO 15118-20, securing all communication to the vehicle with digital certificates is mandatory. This represents a step forward, as in ISO 15118-2 the usage of digital certificates was not mandatory for every functionality. ISO 15118-20 addresses this anomaly being Transport Layer Security (TLS) mandatory for all messaging. Credentials and data signed using a PKI are therefore expected to be adequately protected for tracing the accountability and the integrity of the charging sessions' data and information that are used for billing.

For example, when using ISO 15118-2 PnC service, tariff information is only provided in a relative representation to the EV that may use it for the computation of its optimal charging profile. This requires that the user and EMSP had already established a definition of the absolute values of the charging tariffs. The PKI aims to ensure trust. In the concrete case of PnC, trust is ensured, among other things, by means of digital certificates. However, the PKI is not responsible for the transfer and communicaiton of tariffs, including the relevant information and transparency on pricing.

Advance energy management, load balancing as well as smart and bidirectional charging are key to the integration of electric vehicles into the grid. Existing PKI projects and services (e.g., SAE PKI project) inform about ongoing work to develop basis use cases to reflect this need.

# 3. Identification of PKI projects and services

## 3.1. Description of the scope of the main PKI projects and related-services

**CharIN**

By the time of elaborating this document, CharIN has two communities working on the topic of PKI and PnC.


**Figure 1.** CharIN logo

### 1. Task Force PKI

The task force covers technical discussions and definitions on security topics and interoperability of a CharIN V2G PKI.

A ***Certificate Policy Guideline*** *for the so-called* ***First***[9] *and* ***Second***[10] ***Generation PKI*** has been published in 2022. It gathers the minimum requirements for a dedicated PKI implementation guaranteeing a sufficient level of security. Identification and description of use cases within the PnC ecosystem is currently in progress. These use cases apply to those not yet covered by existing standards and related documents (e.g., ISO 15118-2; VDE Application Guide) to ensure interoperability during the certificates and data exchanges and between multiple actors and ecosystems.

### 2. PnC Project Europe

The goal of the CharIN project "Plug and Charge Europe" is to set up a PKI, a technology needed to enable secure authentication and authorization via Plug & Charge in accordance to ISO 15118, with CharIN as proposed operator and provider of required services. CharIN has presented itself as neutral and international authority that could ensure fairness as well as openness, guaranteeing a level playing field for operating the PKI across all stakeholders. Thus, "Plug & Charge Europe" shall successfully overcome previous hurdles in the implementation. The CharIN V2G PKI aims to enable PnC via ISO 15118 for both versions of the standard ISO 15118-2 and ISO 15118-20.

The team currently consists of 15 active members, namely BMW AG, BP, ElaadNL, EDF, EnBW, Groupe Renault, IBIL, Ingeteam, innogy eMobility Solutions, Porsche AG, Shell Global Solutions Deutschland GmbH, Stellantis, Total, Tritium and Volkswagen AG, and additional supporters.

---

[9] Compliant to ISO 15118-2
[10] Compliant to ISO 15118-20

CharIN PnC Project Europe has published a series of documents, including:

- ***CharIN PKI Price List & Order Form***[11] (December 2022). The document gathers the pricing information, application form for the intermediate CAs and endentity certificates as well as additional information regarding the application process and related documents. Items and prices listed are referring to first-generation V2G PKI certificates according to ISO 15118-2 and second-generation V2G PKI certificates according to ISO 15118-20.
- ***CharIN PnC Europe Governance Guidelines***[12] (May 2022)***:*** The CharIN PnC Europe Governance Guidelines provide a structure within which the CharIN PnC Europe Governance Body and the organization can effectively pursue CharIN's Mission.
- ***CharIN PnC Terms & Conditions***[13] (February 2022). The document aims to provide binding terms and conditions to participate in an open and fair PKI ecosystem for ISO 15118 operated and governed by CharIN e.V., ensuring freedom of choice for consumers as well as a level playing field for its participants.

  CharIN recognises that according to their approach parts of the PnC ecosystem (e.g., pool services, CTL services, other PKIs) would not need to be commercially or technically connected to their CharIN PKI. However, as part of the goal of CharIN to ensure a certain degree of openness and fairness in the ecosystem, the CharIN PnC Terms & Conditions also defined binding Terms & Conditions for ecosystem service providers.

In 2022, CharIN presented a logo of Plug&Charge to help identify the charging points equipped with this service. CharIN indicated that the logo is open to all companies that implement and validate this function in their products in accordance with ISO 15118-2 or ISO 15118-20.


**Figure 2.** Plug and Charge logo elaborated by CharIN

## Gireve

Gireve is a member of the Mobena project and also a service provider whose scope covers Plug&Charge and ISO 15118. Gireve is involved in this sector since 2018.

Gireve is a service provider that currently offers services related to ISO 15118 and PnC: certificates issuing, certificate-authority roles (for V2G Root CA and other RootCA –

[11] CharIN PKI_Price List & Order Form
[12] CharIN PnC Europe Governance Guidelines
[13] CharIN PnC Terms & Conditions Position Paper

operating their own V2G Root CA), and pools management. In practice, these services cover the full scope of the so-called “extended PKI”.

Gireve is offering their own VG Root CA. In particular, Gireve and Thales, a leader in digital security, have collaborated to provide a Plug & Charge access and billing system[14]. The joint solution, based on the Thales Trusted Key Manager and Gireve’s intermediation platform, aims to improve the driver experience, building trust in a multi players’ ecosystem and also helping with the implementation of the ISO 15118 International standard.

Gireve also contributes to several standardisation bodies and specification working groups to develop and promote standardisation, including PnC. In particular, Gireve is member of several initiatives, among which Mobena, to foster the deployment of ISO 15118 and PnC.


**Figure 3.** Gireve logo

**Hubject**

Hubject is operating a functioning PKI since 2018, enabling the productive usage of PnC based on ISO 15118-2. The relevant description on how this solution is working is available for everyone, without lock-in effect, membership or payment in advance via Hubject webpage[15].

Hubject is sharing in their webpage the ***Certificate Policy (CP)*** and the ***V2G Root Certificate***. The CP sets forth the business, legal, and technical requirements governing the use of Hubject’s V2G CA Certificates by participants in the Hubject PKI used for PnC. These materials give also access to additional resources, like the neutral and lock-in free access of the open testing system for PnC, enabling everyone to freely test and implement PnC without any legal connection to Hubject for testing reasons. To ensure the highest level of IT security, Hubject’s V2G Root CA and its PKI operate in a secure Information Security Management System certified with ISO 27001.

In 2022, Hubject presented the ***Open Plug&Charge Protocol (OPCP)***[16], with the goal to standardizing the access of PnC related services. Hubject intends to enable the non-discriminatory free access of the PnC ecosystem for everyone in the industry. Hubject believes this solution is highly needed as the market is continues to adopt PnC and multiple different solutions by organisations emerge. In that context, an open access protocol, without lock-in effects will be needed. Publishing this protocol is for Hubject a key step in enabling this.

Hubject has decided to publish this protocol as open source. To ensure a high level of adoption, protocols published under an open source agreement are the best way to achieve

[14] https://www.gireve.com/product-sheet-plug-and-charge/
[15] https://www.hubject.com/download-pki
[16] https://www.hubject.com/opcp

this purpose and to facilitate a strong collaboration with others. Hubject is keen to joint development possibilities. Hubject invites the whole industry to contribute.


**Figure 4.** Hubject

**SAE EV Charging PKI Project**

The project aims to design and test a so-called inclusive, worldwide EV charging industry PKI platform that is secure, trusted, scalable, interoperable, and extensible. The project is an industry-led, pre-competitive research project to strengthen electric vehicle charging system security. It is based on security industry standards for PKI, digital certificates, and all security industry best practices as well as the experience of industry PKI deployed in other industries.

The project aims to develop a solution that meets the following principles:

- Be agnostic as to charging systems and protocol standards.
- Provide state-of -the-art security based on current industry best practices.
- Define the salient features of the PKI, e.g. certificate structure, required trust anchors rules, policies, and practices a Certificate Authority must follow.
- Be interoperable and extensible to other mobility use cases.
- Be open to use by all ecosystem parties (e.g., automotive manufacturers, charging station vendors, and charging service network operator), provide equal access to a fair and open market, and not limit the number of certificate authorities that can operate the PKI.
- Include an implementation approach that minimizes EV Charging PKI complexity.
- Document all design choices and trade-offs made.

By the end of 2022, the project team completed the design of the ***Draft EV Charging PKI Platform***, including the ***Certificate Policy (CP)*** and the PKI Requirements document. The PKI Platform is including four use cases:

- Mutual authentication between parties, entities and devices using the PKI (e.g. EVs, charging stations, charging service networks) and/or customer.
- Inter-Network Roaming.
- Automated Payment for Services.
- Advanced Charging Energy Management.

The project members inform that there are three other documents included in the technical deliverables: the ***PKI Threat Model***, the ***Industry PKI Review*** and ***Gap Analysis***, including also ***Operationalization Plan Guidelines***. This last deliverable would include a summary of all business decisions needed to be made for the PKI Platform to be migrated into an operational industry PKI.

The project moved to its Testing Phase in January 2022 and it was completed approximately in August 2022. The testing included validation testing of all basic PKI functionality, scalability testing, and adversarial security testing. A project team-only test event was held April 4-7, 2022. Another is being planned for summer 2022.

When all validation testing is complete, the project will be sunset and SAE and the project team members will begin to migrate the PKI Platform to an industry collaborative/consortium and finally an PKI Operating Entity.

At the moment of completing this activity (July 2023), SAE has not shared any of the above-mentioned technical documentation of this project neither with the European Commission nor with the members of the STF Sub-group that are not part of the SAE PKI project.

**Figure 5.** SAE International

**VEDECOM**

The Mobena project gathers 20 partners including 19 industrials. With their stakeholders, they aim to represent the entire mobility sector: Atos, Chargepoly, CRITT M2A, EDF, FEV France, GIREVE, Hager, IES Synergy, Legrand, Nexans, Renault, SAP Labs, Schneider-Electric, Stations-e, Stellantis, Thales, TotalEnergies, Valeo, VINCI Energies. The Mobena project[17] is driven by VEDECOM.

The Mobena project partners are implementing the following actions, in a collaborative framework within working groups:

- Definition of a transition roadmap towards new generation charging solutions and use cases, including PnC and smart charging.
- Creation of technical guidelines for the development, testing and deployment of products and services supporting the ISO 15118 standard.
- Identification and follow-up of pilot projects to test deliverables on the field.
- Dissemination and sharing of the choices with other European initiatives and ecosystems to thrive for a wide adoption and carry the idea of having a replicable solution at the European level.

The main results of the project will constitute a common good which will be made public at the end of the main project milestones.

VEDECOM and Mobena project partners are involved in setting up technical demonstrations to assess interoperability approaches in the charging ecosystem. This collaboration is part of a long-term partnership between VEDECOM and the Dutch innovation center ElaadNL. In this respect, it is worth mentioning the successful ***Certificate Trust List (CTL) demonstrator***[18] carried out on 2 June 2021 as a technical solution for ISO 15118 PnC interoperability. Two online identical sessions were broadcast live from Arnhem (Netherlands), Berlin (Germany) and Versailles (France). The demonstration was operated by 17 actors representing different roles in the Electromobility domain, research institutes, manufacturers, cybersecurity actors, operators, interoperability platforms, charging

[17] https://mobena.org/

[18] https://www.vedecom.fr/e-mobility-a-successfull-demonstration-of-the-certificate-trust-list-for-plug-charge-interoperability/?lang=en

infrastructure installers: Driivz, e clearing.net, ElaadNL, Freshmile, GIREVE, Hager, Hubject, IoTecha, NewMotion, Groupe Renault, SAP, Smartlab, Stellantis, Thales, Trialog, VEDECOM, Verisco.


Figure 6. **Vedecom**

# 4. General definition of possible governance and architecture options

In 2022, there was only currently one operating V2G Root CA (Hubject), with several more V2G Root CAs expected to come into the market by the end of 2022 and beginning 2023 (e.g., CharIN, Gireve, etc.). This scenario carries risks such as non-interoperable market solutions and higher complexity and costs which can strongly decrease the market acceptance of the customer. In this context, the market faces several options for the governance and technical architecture of a PKI.

1) One option would be to strive for **a Single Root CA model**, based on a system which would be fair, open and non-discriminatory, and as such widely accepted by the European industry, where new parties can access the market under clear and equal terms.

2) Another option would be a **Multi Root CA model**, where to guarantee interoperability of existing multiple V2G Root CAs, actors would need to agree on technical, operational and governance aspects of operation. Three technical solutions are possible to ensure interoperability:
   - **Cross Recognition (CR)**: Certificates from different PKIs are signed by each other's certificate authorities in a formal and reciprocal recognition. It ensures interoperability between PKIs by adding additional certificates that can be used to verify a chain of certificates, leading to a different Root CA, without changing the original certificates.
   - **Cross Certification (CC)**: All the PKIs existing in the ecosystem recognise each other as trusted. The path of trust is not hierarchal. Both EVs and charging stations store all V2G Root CAs in their trust store.
   - **Certificate Trust List (CTL)**: It is a predefined list of items that has been signed by a trusted entity. Once the signature of the trusted entity has been verified, the items on the list are "trusted" by the receiver. The CTL can be used to maintain and distribute to EVs and charging stations a list of V2G Root CA certificates that are trusted in the market.

Members of the STF Sub-group believe that strong requirements to the PKI governance would need to be put in place in order to ever reach potential market acceptance in a **Single Root CA model,** notably: integrate the EC in the governance structure, have knowledge organizations as stakeholders and a transparent board of decision makers. In practice, this option would be no longer relevant as multiple actors are committed to offering the service of V2G Root CA.

Therefore, a **Multi Root CA model** is the scenario to be present in the market. Members of the STF Sub-group think that this approach would need to be subject to some extent to EU regulation. The CTL, governed by a Trust List Manager (TLM), is initially considered by members to be the most appropriate interoperability solution that would be compatible with existing products in the market. The TLM manages the PKIs enrolment/revocation process and publishes the CTL which allows the devices to update their V2G Root CA certificates. The TLM role could be executed by a neutral government organization, for example the European Commission, as it is done for the C-ITS.

The CTL solution would help to manage interoperability with V2G Root CAs from inside and outside Europe, and to improve the PKI cybersecurity robustness in case of a V2G Root CA failure. Moreover, having several V2G Root CAs increases the level of security: if case of attack of a V2G Root CA, the whole e-mobility would not be blocked or impacted, but only the "scope" of the compromised V2G Root CA(s). The ability of having several V2G Root CAs is also a important principle to avoid any monopoly situation, to ensure a open and free market, and thus to reduce costs and prices driven by competition.

In addition to the governance of the V2G Root CAs, it is of interest also to consider the question of the governance of multiple 'PKI ecosystems' (aka 'extended PKI') and their interoperability. A PKI ecosystem can be understood as the complementary actions of the PKI to manage, for example, PnC contract certificate provisioning. Members believe that the PKI ecosystem should cover at least the following technical roles: ***PCP (Provisioning Certificate Pool)***, ***CPS (Certificate Provisioning Service)***, ***CCP (Contract Certificate Pool)***. The actors managing and offering PKI ecosystem roles may or may not be the same ones managing the PKI V2G Root CA. They may manage and offer PKI ecosystem roles and services for one or multiple PKIs. Multiple PKI ecosystems may operate on the same market. Their interoperability should be guaranteed for basic services at least. In addition, they may offer different kinds of services based on their own business models.

Members of the STF Sub-group expressed the following views on the governance of multiple PKI ecosystems:

- According to *Mobena*, the governance at the European level should only apply to the e-mobility PKIs covering V2G CAs, particularly the CTL and the Trust List Manager (TLM). PKI ecosystems, services and actors may be excluded from the governance scheme.
- According to *CharIN*, their Plug and Charge Project Europe Governance Guidelines (see section Block 1, Point 2) provide a structure within which the CharIN V2G Root Governance Body and the organization can effectively pursue CharIN's mission. The CharIN V2G Root Governance Body intends that these Guidelines serve as a flexible framework within the CharIN V2G Root Governance Body under wich to conduct its business, and not as a set of binding legal obligations. These Guidelines should be interpreted in the context of all applicable laws, policies, and processes. All industry members are encouraged to join.

In November 2019 AFIREV published a position paper entitled ***Recommendation on communication security for roaming electric vehicle charging***[19] focused on potential PKI architectures related to ISO 15118.

In this analysis, four PKI architecture models are described, analysed and compared:

- **Unique Non-regulated Architecture (UNA)**: A unique, market-based authority. In this architecture, the unique V2G Root CA is a commercial actor who is the sole manager of the certification system (in its governance and IT implementation) and who is responsible for its operation and interoperability. It therefore lays down the operating rules.
- **Unique-Regulated Architecture (URA)**: A unique authority regulated at European or international level. In this architecture, the unique V2G Root CA is a non-commercial actor regulated by a public authority (either a European regulatory authority or a consortium of private actors regulated by a European authority). This V2G Root CA can be divided into three parts:
  - Governance (we will call it V2G Root CA - "Regulatory Authority"): sets the rules of governance and applies them in an unambiguous way. It is the owner of the private key of the V2G Root CA and is responsible for the proper functioning of the certification system.
  - Certification operation (we will call it V2G Root CA - "Certification System Manager"): elected following a call for tenders issued by the V2G Root CA - "Regulatory Authority", it manages the IT system. By complying with the standards in force and the additional requirements of the regulatory authority.
  - Audit (we will call it V2G Root CA - "Auditor"): selected following a call for tenders issued by V2G Root CA - "Regulatory Authority", it audits the V2G Root CA - "Certification System Manager" (audit to be made public).

[19] https://www.afirev.fr/wp-content/uploads/2019/11/AFIREV_Reco_PKI_ISO15118_2019-En.pdf

- **Multi Non-Regulated Architecture (MNA)**: A federation of cross certifications. In this architecture, there is not one but several V2G Root CAs that coexist and whose legal structure is not imposed. Each V2G Root CA manages its own certification chain in a way comparable to UNA or URA architectures. In order to ensure system interoperability, a bilateral link between V2G Root CAs is necessary. Each V2G Root CA selects its own trusted V2G Root CA. Technically these bilateral agreements could be implemented via a Trust List mechanism or via a cross-certification mechanism.

- **Multi Regulated Architecture (MRA)**: A bridge administrative authority. As in the MNA architecture, there is not one but several V2G Root CAs that coexist and whose legal structure is not imposed. Each V2G Root CA manages its own certification chain in a way comparable to UNA or URA architectures. However, unlike the MNA architecture, system interoperability is managed by an administrative authority whose mission is to create a unique list of trustworthy V2G Root CA (this list is named "Trust-List of V2G Root CA"), maintain it and publish it. This authority sets minimum governance requirements and rules that must be respected by any new V2G Root CA wishing to join the trust list to be interoperable. In order to verify compliance with these minimum governance rules, the administrative authority publishes specifications and requirements and calls upon specialised audit actors to audit new applicants and manage the list of members.

The analysis and comparison have been based on the following seven criteria:

1. **Transparency of the V2G Root CA**: Accessibility to info related to governance rules, pricing, terms and conditions, etc.
2. **Distribution of V2G Root CA functions**: Activity and responsibility split between Governance, Operation and Audit.
3. **System interoperability.**
4. **Complexity of implementation and deployment**: complexity and effort to set up the PKI architecture.
5. **Existence of barriers to entry for a new V2G Root CA.**
6. **Scalability of the system.**
7. **Economic and technical resilience of the V2G Root CA**: The resilience of a system is its ability to overcome rare and disruptive events without impacting its service level.

The analysis can be summarised in the following table (for more details, see the original document – footnote 19):

| | | UNA | URA | MNA | MRA |
|---|---|---|---|---|---|
| | | **Unique non-regulated** | **Unique regulated** | **Multi- non-regulated** | **Multi regulated** |
| **1** | **Transparency** | *T*=Can change rules and conditions etc. at any time<br>W=No competition & Anti-trust pb | S=Governance rules are established and evolve through regulation and are therefore known to all. | *T*=V2GRootCA can change rules and conditions at any time<br>*S*=Players can choose their V2GRootCA<br>O=Competition is active | S=Set of mandatory rules to be respected by all V2GRootCAs<br>S=Governance rules are specific to each V2GRootCA (open market and competition)<br>S=Players can choose their V2GRootCA<br>O=Competition is active |
| **2** | **Function Distrib.** | *T*=No "real" audit is possible | *O*=A separation can be set up between Governance, Operational management and Audit | *T*=No "real" audit is possible | S=Audit is based on external and common rules. Audit is in place and contributes to transparency |
| **3** | **Interoperability** | S=Interoperablity is easy<br>T=High discrimination potential | S=Interoperablity is easy | *W*=No interoperability by default<br>*O*=TrustLists or CrossCertif could improve Interop<br>*T*=Interoperability depends on V2GRootCA goodwill | S=Interoperability is managed by a neutral actor and don't depend on players goodwill |
| **4** | **Set-Up complexity** | S=No complexity | *T*=Complexity is focused on gouvernance Set-Up and lifecycle | *W*=TrustLists (several) implementation could be long/complex | *T*=Complexity on gouvernance set-up and lifecycle<br>*T*=Addition of a new actor (TrustList Manager)<br>*O*=TrustListManager is an already existing role, at least for C-ITS |
| **5** | **Barriers** | *W*=Creating a new V2GRoot is, by definition impossible | *W*=Creating a new V2GRoot is, by definition impossible | *S*=New V2GRootCA creation is easy<br>*T*=Trust negociation with other V2GRootCA could be dificult/impossible and avoid any interoperability | S=New V2GRootCA creation is easy<br>S=Conditions for entering the "interop. Area" are clear, transparent and non-discriminatory |
| **6** | **Scalability** | *W*=No "horizontal scaling" or volume distribution between several V2GRootCA | *W*=No "horizontal scaling" or volume distribution between several V2GRootCA | *S*=Volume distribution between several V2GRootCA | S=Volume distribution between several V2GRootCA |
| **7** | **Resilience** | *T*=The unique V2GRootCA is a "single point of failure". A cybersecurity incident, or Bankrupcy could impact the whole "Plug&Charge" ecosystem | *T*=The unique V2GRootCA is a "single point of failure". A cybersecurity incident could impact the whole "Plug&Charge" ecosystem | *S*=No "single point of failure". A cybersecurity incident, or Bankrupcy will impact only a part of the eMobility ecosystem<br>*T*=because interop is based on bilateral agreement, a pb with one actor could have a domino effect | S=No "single point of failure". A cybersecurity incident, or Bankrupcy will impact only a part of the eMobility ecosystem |
| | | *S="Strength"* *W="Weakness"* *O="Opportunity"* *T="Threat"* | | | |

Based on this analysis, AFIREV's recommendation is to deploy the "***Multi-V2GRootCA Regulated Architecture***" (MRA). AFIREV also indicates that the "Unique-V2GRootCA Regulated Architecture" (URA) might be acceptable, due to its positive governance characteristics and because it is "easy to deploy", but scalability and resilience should be strongly improved.

AFIREV also highlights the fact that, even if the interoperability of V2G Root CAs could be solved by both cross-certification method and trust-list mechanisms, cross-certification could be a good solution for a governance based on V2G Root CA bilateral agreements. However, **a trust-list mechanism should be the best solution for a central governance**.

# Block 2: Identification of a high-level framework for the functioning and operation of a PKI ecosystem in the EU

SUSTAINABLE TRANSPORT FORUM

# Block 2: Identification of a high-level framework for the functioning and operation of a PKI ecosystem in the EU

This part of the document outlines the **preferred PKI governance and architecture framework by the members of the STF Sub-group on Governance and Standards** for the set-up and future operation of an interoperable EU PKI ecosystem in the EU. The proposed framework is made up of the recommendations provided by the main PKI project developers and service providers (Block 1, point 2), considering also the views and additional policy and technical challenges indicated by other participant members of the STF Sub-group. For that, these members engaged with the EC and PwC during regular meetings of the STF sub-group and Phase 1 of the Commission Support Study.

The proposed framework represents a high-level approach to the topic, identifying first the key strategic governance, architecture and implementation elements that require a concrete position by industry stakeholder before moving to a Phase 2, where the definition of a joint implementation takes place. The framework presented here duly considers the needs of the different market players and feature quantifiable arguments, why to be chosen.

During this section, the different high-level options are identified and explained. For each option, the concrete position of those STF members who wish to add their specific point of view is reflected, concluding at the end a common recommendation by the whole STF Sub-group that allows to move the topic forward. This approach responds to the need to accelerate this discussion at a point where the electromobility market enters a critical roll-out phase. All members have been encouraged to establish bilateral discussions and reach consensus based on mutual compromises for the sake of ensuring the development of a united EU electromobility market based on high-quality services.

In practical terms, **a total of six high-level areas** have been identified that would require a clear position in order to lay down the basis for a common PKI framework to this topic. These areas are summarised below and elaborated throughout this section with the formulation of joint recommendations. These six areas aim to provide a robust framework where the main regulatory, governance, architecture, ownership and implementation aspects are agreed.

- **Recommendation 1:** A regulated or a non-regulated governance and architecture approach.
- **Recommendation 2:** A Single or a Multi Root CA model
- **Recommendation 3:** Interoperability
- **Recommendation 4:** Governance model
- **Recommendation 5:** Ownership model
- **Recommendation 6:** Implementation scheme

Importantly, these recommendations and the high-level framework concluded will need to be further elaborated in order to support a subsequent market implementation. This is a natural and necessary first step before moving towards concrete technical discussions that

are only possible when all stakeholders coincide on the same technological principles and solutions.

## 1. A regulated or non-regulated governance and architecture approach

When something is systemically important to society and may cause systemically important disruptions, this brings attention from governments and regulators. The implementation and usage of PKI systems in the electromobility sector implies a systematically important situation that affects multiple stakeholders (e.g., OEMs, CPOs, DSOs) and end users. In Europe there are approximately 250 million passenger cars on the road, with more than 300 potential EV drivers. Consequently, the future use and interaction of PKI related services for recharging of electric vehicles is a matter that would not go unnoticed by the legislator.

All industries are somehow subject to general legislation, with some also having industry-specific legislation. Traditionally, this is the case of the automotive industry, where different parts of the industry are regulated by sectoral legislation. In the case concerning this expert group, alternative fuels infrastructure is addressed. Likewise, other possible links affecting electric vehicle and recharging infrastructure are investigated, such as access to in-vehicle data or vehicle type-approval.

On that basis, **there is a clear benefit on the development of a specific regulatory approach for electric vehicles and charging infrastructure that brings certainty and common requirements for the future operation and interoperability of the preferred governance and architecture for a PKI ecosystem in the EU**. Standards, technical interoperability, security or fair competition, these are all important aspects that would benefit from regulatory certainty.

At the same time, there exist certain aspects that are understood to be better left to the market as a business area. In any circumstance, a specific regulatory approach in this field should aim to prevent unfair practices by one or several industry actors that could lead to market foreclosure and work against the user interest.

**Recommendation 1: A regulated vs. non-regulated governance and architecture approach**

Members of the STF Sub-group on Governance & Standards agree and **recommend a regulated approach for the PKI** ecosystem governance and architecture in the EU. This regulated approach should be characterised by the agreement and backing in legislation of a series of minimum policy, technical and operational requirements aimed at ensuring an open, interoperable and competitive PKI system.

Members of the STF Sub-group on Governance & Standards are willing to work together and with the EC to identify, elaborate and conclude those concrete requirements that could be included in legislation.

# 2. A single or Multi Root CA model

An open an interoperable PKI for electromobility can be achieved in different manners. The market design can be based on a Single or Multi Root CA model. The market design can also differ in different regions of the world, for example in Europe, North America or Asia.

The development of a **Single Root CA model**, based on a system which is fair, open and non-discriminatory, requires that all participant stakeholders recognise a single actor as Root CA. Considering several STF Sub-group members views this would require to integrate the EC in the governance framework or to develop a hard legislation to ensure a widely acceptance by the whole European industry, where all parties would have the certainty that could access the market under clear and equal terms. Today, this option is no longer relevant as multiple actors are already committed to offering the service of V2G Root CA (e.g., CharIN, Hubject, Gireve).

The **Multi Root CA model** becomes the natural design based on several market actors decision to offer V2G Root CA services. To guarantee interoperability of multiple existing V2G Root CAs, market actors would need to agree on technical, operational and governance aspects of operation. The existence of several V2G Root CAs is considered an important principle to avoid monopolistic situations, facilitating an open and free market directed towards reduced costs and prices driven by competition. Finally, the operation of several V2G Root CAs has an additional positive aspect: it increases the level of security and operational resilience. In case of attack of a V2G Root CA, the whole electromobility would not be impacted, but only the “scope” of the compromised V2G Root CA(s).

However, a Multi Root CA model could also add on the negative side a layer of complexity and cost. To this respect, interoperability is considered essential and should be ensured for the entire ecosystem. One aspect to take into account is the case where a European EV manufacturer may export their vehicles to a foreign market. Here, global interoperability between trusted Root CAs would be crucial for the scale up and roll-out of electric vehicles beyond EU borders. This aspect would be a challenge that the EU PKI ecosystem would have to address as a whole.

**Recommendation 2: Recommendation on a Single or Multi Root CA model**

Members of the STF Sub-group on Governance & Standards agree and **recommend a Multi Root CA model** for the PKI ecosystem governance and architecture in the EU.

This option corresponds to a situation where multiple market actors are already committed to offering the service of V2G Root CA (e.g., CharIN, Hubject, Gireve) in the EU.

Members of the STF Sub-group on Governance & Standards are willing to work together and with the EC to determine clear requirements on interoperability to ensure the best functionality and secure the ecosystem so that any vehicle works with any recharging station. To materialize vehicle-infrastructure compatibility under multiple Root CAs, members consider particularly important to provide legal certainty around the protocols and standards that the industry shall apply as minimum mandatory requirements.

# 3. Interoperability across Multi Root CAs

As introduced in the previous recommendation, **interoperability between multiple V2G Root CAs is key**. Imperatively, to ensure market interoperability of existing multiple V2G Root CAs, relevant market actors will need to agree on technical, operational and governance aspects about the functioning of multiple V2G Root CAs. These aspects could be afterwards defined and backed up in European legislation given certainty to the future PKI for e-mobility in the European Union.

In practice, there exist three technical solutions for the interoperability of multiple V2G Root CAs (Cross Recognition – CR, Cross Certification – CC and Certificate Trust List – CTL)[20]. In line with Phase 1 of the Commission Support Study these solutions were investigated. PKI project and services providers were specifically interviewed on the status of their projects and overall position on this matter. The following conclusions were reached:

- PKI providers were working to reach commercial roll-out. In terms of interoperability, most PKI projects were currently testing solutions in order to be ready to implement them as soon as the necessity arises in the market.
- PKI providers generally agree on the need of determining convergence towards a single interoperability solution as soon as possible.
- To reach interoperability, market actors should reach the same level of trust between their Root CAs. This might be fostered through standardization (e.g., broader adoption of ISO 15118).
- There exists a general preference of PKI providers towards the **CTL interoperability solution**. The advantages include scalability, ease of operation and set-up, easier maintenance and compatibility with the current ISO 15118-2

[20] CR, CC and CTL were outlined in Block 1, Point 2.

and -20, adequate logic of the certificate verification (algorithms, software, etc.). As main disadvantage, the CTL will likely imply a slower implementation time, with the need of a Trust List Manager (TLM).

- **Cross Recognition (CR)** and **Cross Certification (CC)** may result in faster implementation due to higher simplicity. However, scalability could be a limiting problem that could hamper the EU-wide implementation of these solutions in the number of Root CAs reaches a certain number. This could lead to market fragmentation, including several interoperability solutions in place.
- Co-existence of multiple interoperability solutions would be technically possible, but certainly undesired as it may lead to islands in a fragmented market. There is a common view on the need to reach an agreement on PKI interoperability in early stages, namely at present.

The conclusions described above can be further complemented with the individual positions and concrete view of the PKI providers (and other industry members).

- *CharIN* believes that Cross Recognition (CR) and Cross Certification (CC) might be two valid alternatives worth exploring. However, it is open to provide support to other solutions, including CTL.
- *Gireve* thinks that CTL is the most suitable option.
- *Hubject* supports the establishment of a neutrally operated Certificate Trust List Manager (CTL). The V2G Root CA operator shall not be involved in any business related service regarding ISO15118, PnC or other potential PKI related services to ensure a full neutrality. Hubject provides the summary displayed below where the different options are compared.

| Issues addressed | Maintainability | Technical feasibility | Scalability | Where is interoperability handled? |
|---|---|---|---|---|
| **Cross recognition** | - "Root Certificate Pool" useful in case of many PKIs.<br>- Revocation = removing a V2G Root certificate directly from trust store (CRL cannot be used) | - Confirmed<br>- Possible with ISO 15118-2 / -20 | - If n PKIs -> n V2G Root CAs installed in EV and Charging Station<br>- On boarding effort is once per additional root CA | - Interoperability handled "inside" the EV (for installing CC and setting up TLS to Charging Station) and EVSE (for authorizing the CC) |
| **Cross Certification** | - Perhaps a "Cross Certificate Pool" needed in case of many PKIs?<br>- Revocation: add cross certified V2G Root CA to the CRL of the cross certifying V2G Root CA. This is standard way of handling CRLs. | - Yes, as shown in webinar / demo July 2020<br>- Possible with ISO 15118-2 with PKI hierarchy layer limitation (see 5.1).<br>- Possible with ISO 15118-20 (based on current draft) | - If n PKIs -> max n(n-1)/2 cross certificates in Charging Station and CCP, only 1 in EV during certificate installation and setting up TLS connection<br>- On boarding effort per additional cross certification relation | - Interoperability is handled "outside the EV" (at the EVSE / PnC ecosystem)<br>- Cross certification entails a bilateral trust relation between independent PKIs and therefore requires the governance rules to take this "per actor"/ bilateral character into account |
| **Certificate Trust List** | - CTL manager maintains list, maintenance is part of CTL mechanism.<br>- Revocation = removing a V2G Root certificate from CTL (CRL cannot be used) | - Yes, as shown in webinar / demo June 2021<br>- For infrastructure route: possible with use of a Value Added Service (VAS) or other extension to ISO 15118.<br>- For telematics route: no impact on ISO 15118 | - If n PKIs -> n V2G Root CAs from CTL installed in EV and Charging Station<br>- Identical to cross recognition<br>- On boarding effort is only once per additional root CA | - Trust List Manager<br>- This has an association with "central governance", due to the role of the central Trust List Manager that has to trust a PKI in order to add it to the CTL. |

**Figure 7.** Comparison of PKI interoperability options (Source: Hubject)

- *SAE* has no position.
- *Vedecom* supports a CTL as the most appropriate interoperability solution considering compatibility with existing products in the market. Overall, Vedecom believes that is important to reflect that the PKI interoperability may be industry-

driven or government-driven. Technical solutions could be adapted to each approach. Concretely, Vedecom recommends a Multi Root CA model with a CTL architecture wihere the TLM is government-driven, for example the European Commission could perform this role as it is currently done for the C-ITS. Vedecom provides the summary displayed below where the different options are compared, indicating the recommendatiojn of Mobena project.

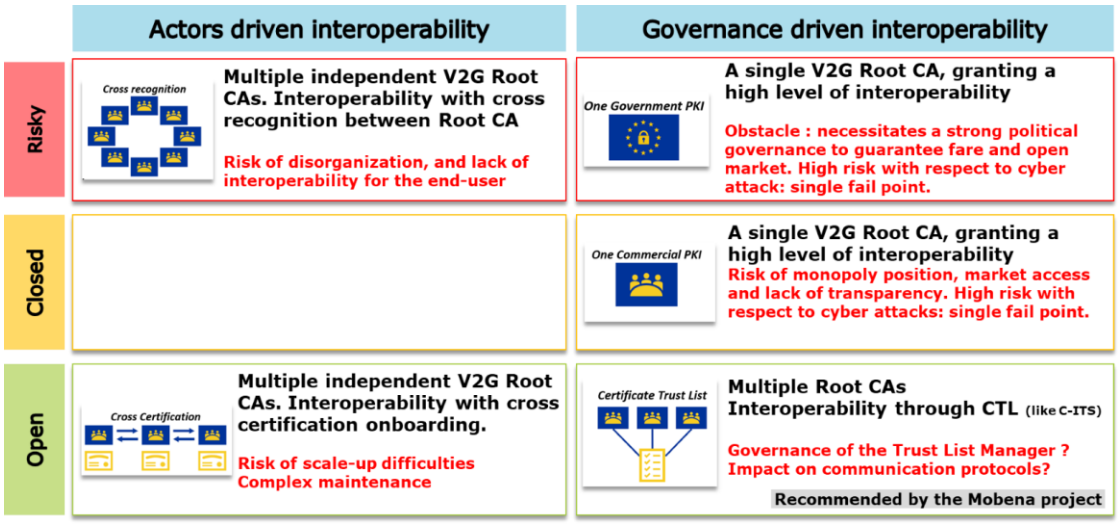


**Figure 8.** Comparison of PKI interoperability options (Source: Vedecom)

The preferred interoperability solution, CTL, requires the involvement of several actors, covering different roles (e.g., body in charge of publishing and maintain trust list –Trust List Manager), supervised by a neutral authority.

The role of the Trust List Manager may be covered by the EC (or a delegate) or by an industry consortium (subject to EU legislation). There is a preference towards the EC as it would ensure neutrality and the joint representation of the interests of the different actors in the market. By contrast, the advantage of an industry-driven approach is that it allows a more dynamic organization based on specific business developments. Conversely, an uncontrolled growth in the number of actors (V2G RooT CAs) might pose limiting issues to the operation and quality of the system. In this respect, both Cross Recognition (CR) and Cross Certification (CC) could somehow sustain the growth of the market but not the increase in number of PKI providers as it will result in exponential complexity being generated. However, having more than 3-5 V2G Root CAs will render the whole CR or CC system impossible to manage.

**Recommendation 3: Interoperability across Multi Root CAs**

Members of the STF Sub-group on Governance & Standards show a general preference and r**ecommend interoperability across Multi Root CAs by means of a Certificate Trust List (CTL) architecture** managed by the EC. This is due to its advantages, particularly ease of operation and set-up, easier maintenance and compatibility with the standard ISO 15118-2 and -20 and suitable logic of certificate verification (algorithms, software, etc.)

CharIN points to Cross Certification (CC) as a plausible alternative, given its ease of operation and higher simplicity, however, the number of Root CAs might be a limiting factor affecting the overall scalability and operation of the PKI. CharIN is therefore also open to contribute and provide support to the CTL interoperable architecture.

Members recommend a CTL structure that involves actors from the both industry and government within the PKI with a neutral authority, in the specific case of the CTL, overseeing this process. Moreover, it is recommended to allow the industry to organise itself. The EC should be the "vision owner", briging actors together, setting up the legal requirements and providing technical support (e.g., PKI CTL set-up).

Members recommend a market push for the standard ISO 15118 as the minimum common technical standard, including a mandate in EU legislation (i.e., AFIR secondary legislation) based on clear and reasonable timeline for the adoption of -20. This standard should be compatible with other standards and protocols to ensure the functioning of the overall PKI infrastructure.

Members of the STF Sub-group on Governance & Standards are willing to work together and with the EC to identify and elaborate those minimum requirements needed to establish a PKI interoperable model in the EU under a CTL architecture (e.g., criteria that allow the verification of the trustworthiness of V2G Root CAs and Sub-CAs, market rules, additional standards and techncial aspects, etc.)

# 4. Governance model

**The governance model is an essential part of the PKI ecosystem**. Governance of IT systems typically ensure the effective and efficient use of technical systems in enabling an organization to achieve its goal. Such an organization may serve different purposes. Proper governance will ensure that any changes introduced are mutually recognized, well understood, carefully considered, and are effectively communicated to the community of trusted parties.

Depending on the project use case, there exist possible alternatives for the governance model of a PKI. In line with Phase 1 of the Commission Support Study the possible governance options were investigated. PKI providers were specifically interviewed on this matter. As a result of this analysis, a total of up to 7 different governance options were identified for the e-mobility PKI. What differs, and defines the 7 different government

options, is the actors covering the roles within the governance framework: business organisations, industry consortium, public authorities or a mix.

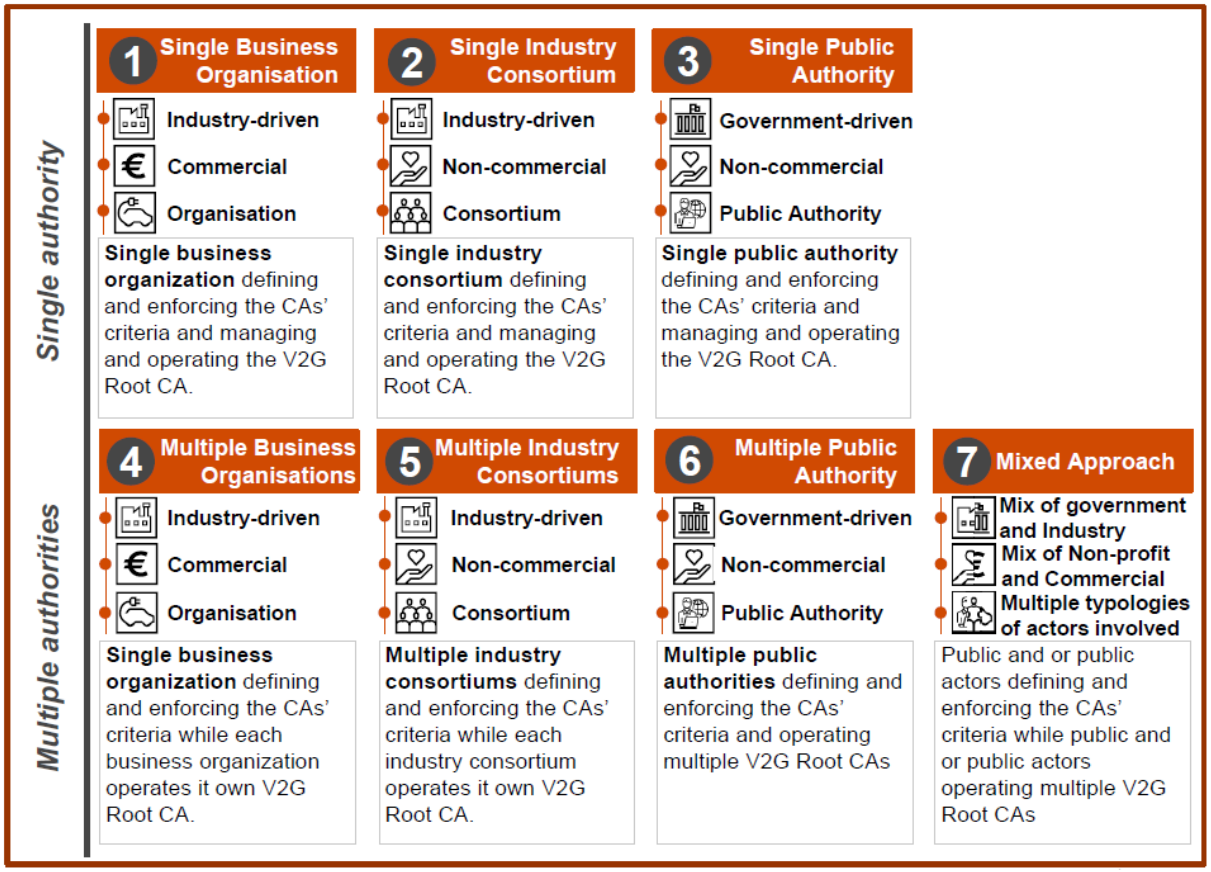


**Figure 9.** Governance options for the PKI (Source: PwC)

The **mixed approach** results in the preferred option by PKI providers. It foresees the EC setting up the criteria for V2G Root CAs to be considered trustable and defining the governance rules (i.e., auditing procedures). This relates to the ability to impartially grant a fair, open, and non-discriminatory access to the PKI as well as for being widely accepted in the market.

Under any interoperability solution chosen, there are two governance layers that need to be developed in any case: i) the definition of a mutually accepted set of criteria for the trustworthiness of CAs, ii) the check of criteria compliance of CAs. The concrete case preferred of CTL features an additional governance layer: publishing and management of the list of trusted CAs.

**Recommendation 4: Governance model**

Members of the STF Sub-group on Governance & Standards show a general preference and recommend a PKI governance approach based on a "**mixed approach" option**, where one public authority (or several public authorities – also possible) is in charge of the **governing level** (criteria for CAs trustworthiness and governance rules) and the commercial actors are responsible for the **operational level**, namely managing and operating the certificates exchange.

When it comes to the **CTL interoperability model**, there are three governance layers to consider. First, the definition of a list of common criteria. Second, the checking of the compliance of CAs against that set of criteria. Third, the publishing and management of the list of trusted CAs. Members recommend to work in the definition of a mutually agreed set of criteria for the acceptance of a neutral governing authority.

More generally, members of the STF Sub-group on Governance & Standards are willing to work together and with the EC to discuss and define the specific actors, sub-roles and sub-tasks within the governance model, especially when it comes for V2G Root CAs. In addition, other policy and legal elements to underpin the proposed governance model are also recommended to define. In this respect, there is the need for the adoption of a common Certificate Policy (CP) template containing the minimum requirements to be implemented by each V2G Root CA, and Certificate Policy provisions (e.g., revocation policy, security policy, auditing policy, etc.)

Finally, members recommend that the proposed PKI governance framework is developed and discussed in the context of the Alternative Fuels Infrastructure Regulation (AFIR) and through the STF Sub-group on Governance and Standards. This could then be eventually introduced in EU law through a Delegated/Imeplementing Act.

# 5. Ownership model

One of the crucial questions in a PKI system is: who should cover the roles and responsibilities within the PKI ecosystem?

The ownership model of the PKI is understood by members of the STF Sub-group as the definition of the owners of each role and responsibility to be covered by the different actors within the ecosystem. Key roles of the PKI includes: definition of the key rules and criteria to recognize as trustable the other actors within the PKI, the compliance checking process of the criteria and the publication of the results of the compliance checking process. In addition to this, there are other roles and responsibilities, covered by different ancillary actors within the ecosystem.

In line with Phase 1 of the Commission Support Study the ownership model was investigated and PKI providers as well as other interested members were specifically interviewed on this matter.

It was possible to ascertain that all the roles and responsibilities would need to be performed by one or more actors. More especifically, organisations covering roles at **governing level** should be non-profit and certify their conformity against a set of requirements and, in terms of legal obligations, they should be open and non-discriminatory towards the other actors within the PKI ecosystem. The organisations covering roles at **operating level**, in general, do not require specific organisational requirements but should be highly trustable as well, in terms of legal obligations, should be non-discriminatory, imposefair pricing and be compliant to competition rules.

Importantly, a series of key roles and responsibilities for both the governing and operating level were also identified. These roles and responsibilities were also linked to main actors and potential legal obligations.

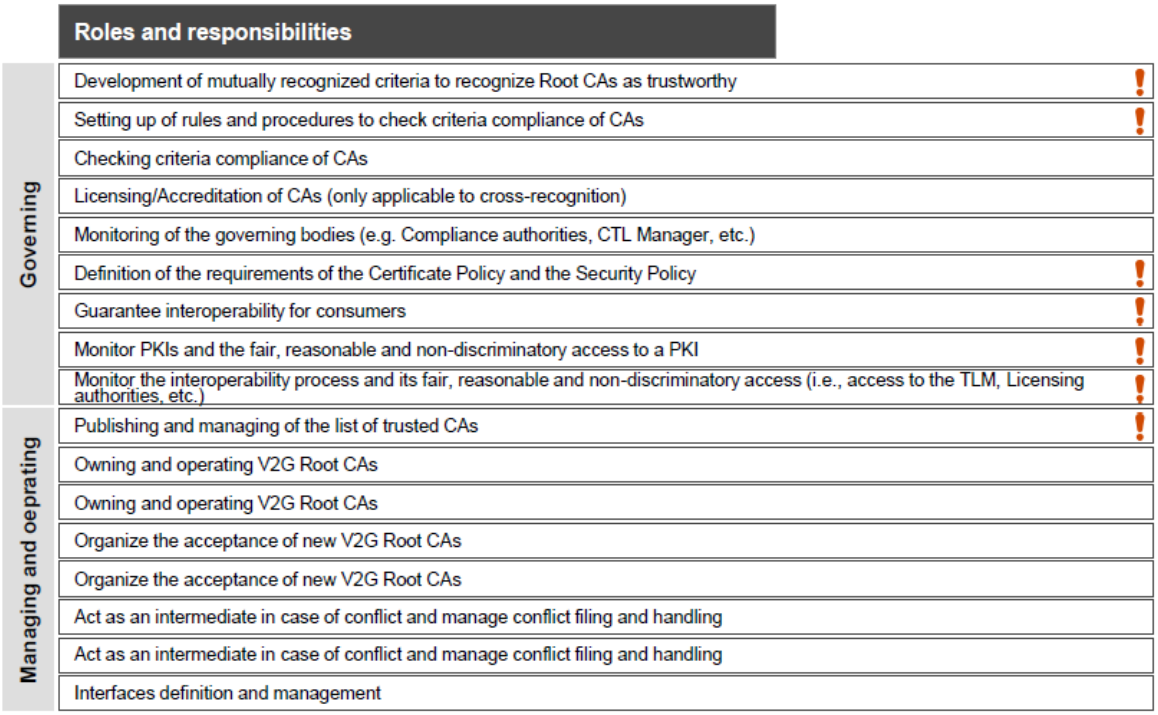


**Figure 10.** Roles and responsibilities PKI (Source: PwC)

Finally, linked to the ownership it must be also explored the associated revenue model, including the cost and fees charged to users. In this respect, the revenue model structure can take various forms subject to subscription fees but also other aspects, such as certificate generation or access to pools.

The future financing of a public authority (e.g., European Commission) to carry out the roles within the governing layer could be achieved through exclusively public funding (e.g., Connecting Europe Facility, CEF) or through a (partial/total) cost-covering fee (e.g., tax) applied to participants in the PKI ecosystem. When applying a tax the subjects to which the fee is applied need to be defined in a fair and clear way. The European Commission as public authority in discussion with industry participants would determine the amount of that cost-covering fee.

**Recommendation 5: Ownership model**

Members of the STF Sub-group on Governance & Standards recommend that **in the PKI ecosystem for e-mobility several roles can and should be covered by for-profit organisations (i.e, owning V2G Root CAs, criteria compliance check, etc.) but must be performed respecting the rules set up at governance level**. Here, the high-level governing roles should be performed by a trusted, neutral, accepted, open and non-discriminatory organisation. For this reason, the general preference is to leave this role in the hands of a public authority (e.g., EC).

Members recommend the development of a series of mechanisms to ensure a fair, open and non-discriminatory access to the PKI. These include:

- Putting in place a sound approach for data portability with a seamless transition among operators.
- Adoption of common APIs.
- Definition of access conditions to other PKIs and the set of trusted actors that are accepetd in the ecosystem.
- Definition of market rules.

Finally, members recommend that **transparent operation of V2G Root CAs is pursued with a combination of technical requirements** (i.e., minimum requirements and publishment of CP and CS), **market rules** (i.e., CPS and resilience plan) and **EU legislation** (i.e., obligation of application of technical requirements and market rules) with a specific focus on security and scalability.

# 6. Implementation scheme

Implementation can be costly and time consuming. If not done in a smooth manner, incremental costs could be transferred to end user leading to unattractive services.

In a future EU PKI ecosystem, the preferred interoperability option (i.e., CTL) would have to be paired with an ad hoc version of the Certificate Policy (CP) requirements. For this specific reason, reaching a common agreement on the preferred interoperability option and the path to implement it is of utmost importance.

In line with Phase 1 of the Commission Support Study the implementation model was investigated and PKI providers as well as other interested members were specifically interviewed on this matter.

The results indicated that Cross Certification (CC) would be the interoperability option with the highest readiness for implementation. The CTL, regardless being behind form a standard and technical specifications point of view, could make up the gap quickly thanks to the best practices available in other sectors (e.g., C-ITS). The CTL although it may require a higher initial economic and workload investment in comparison to the other interoperability solutions, it counterbalances this issue with lower operating costs and higher capability to support the expected growth of the market.

In terms of implementation roadmap, the full implementation phase would entail the set-up of the preferred interoperability option to support the expansion of the market. Expansion is expected to be two folded. On one side the e-mobility market is expected to experience a flood of new EV drivers. As a consequence, the e-mobility market players – non only PKI operators but also EMSPs, CPOs, etc. – could be expected to grow in size and number to accommodate them. In that scenario, it would begin urgently the implementation of the interoperability solution that has been reached.

Theoretically, the chaotic situation described above should be avoided, and market actors should agree beforehand on a PKI interoperability solution that is set-up in due time, ideally from early stages of commercial PKI solutions for e-mobility.

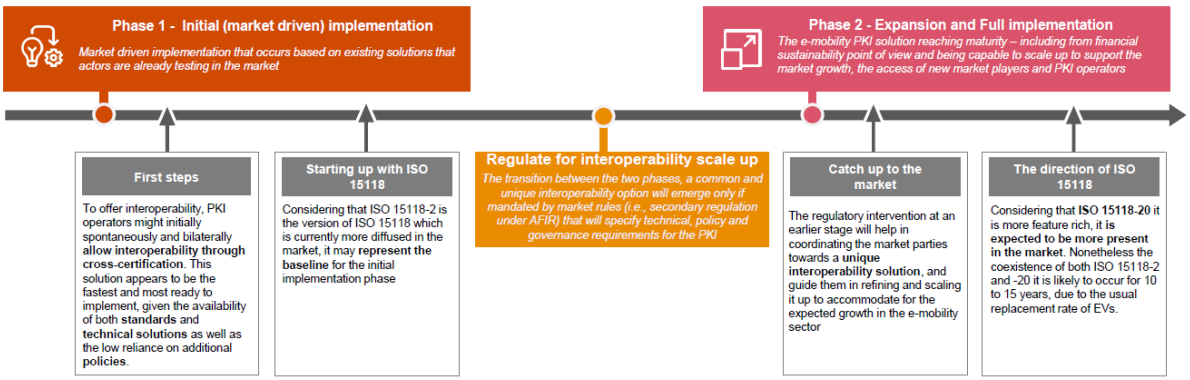


**Figure 11.** Proposed implementation scheme leading to a EU PKI ecosystem

**Recommendation 6: Implementation scheme**

Members of the STF Sub-group on Governance & Standards belive that In order to implement a PKI interoperability solution, two phases should occur. The **1st phase** would be **market-driven**, based on existing solutions that market actors are already bringing to the market. Then, a **2nd phase** would take place, where **a common EU PKI interoperability solution – the CTL approach - would be implemented**, subject to agreed market rules and a series of legal provision established in legislation (i.e., AFIR delegated/implementing acts).

# Block 3: Identification of regulatory needs and other outstanding technical aspects

SUSTAINABLE TRANSPORT FORUM

# Block 3: Identification of regulatory needs and other outstanding technical aspects

In Activity 1 (see Mapping of the discussion concerning standards and protocols for communication exchange in the electromobility ecosystem)[21] of the STF Sub-group on Governance and Standards, several follow-up topics within the discussion concerning standards and protocols for communication exchange in the electromobility ecosystem were identified.

These topics concern from general problems such as how to synchronize relevant European legislative acts addressing recharging infrastructure and EVs, to specific issues in relation to standards such as ISO 15118. In practice, to elaborate these topics in a structured manner in Block 3, the issues described are grouped around four principal thematic areas. Within each area, the relevant issues are presented and concrete recommendations are proposed by members of the sub-group on how the European Commission as regulator could solve them.

The four thematic areas are:

1) PKI, Plug & Charge and ISO 15118
2) ISO 15118 – User access to functionality and smart charging
3) Data sharing
4) Standards, mandates and conformance.

## 1. PKI, Plug & Charge and ISO 15118

### 1.1. Interoperability and accessibility for multiple PKIs (and certificates)

**Context:**

Interoperability, accessibility and portability between different systems and service providers is crucial and therefore frequently referenced in government policies, especially in the EU.

The members of the STF Sub-group endorse on the following important principle:

*Technically any EV-driver must be able to charge any EV (whatever the car maker), on any (publicly accessible) charging station (whatever the charger maker, whatever the CSO, whatever the country in Europe), using any service provider (whatever the EMSP). This principle and this goal imply certain "universal" common requirements, on a technical level and on the policy level.*

[21] European Commission, Directorate-General for Mobility and Transport, Mapping of the discussion concerning standards and protocols for communication exchange in the electromobility ecosystem, Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2832/6763

This principle does solely focus on the technical aspects and does not necessarily mean for mandatory e-roaming between all EMSPs, CSOs and e-roaming platforms in EU legislation. However, to enable reliable charging processes, commercial e-roaming agreements between EMSPs and CSOs are needed. To realize this goal, different levels of interoperability between the mentioned actors are needed:

***Interoperability on a technical level:***

Interoperability on a technical level implies that the "system" (the IT system and the organization around it) of any actor must be able to collaborate with the "system" of any of its counterparts. This is what members jointly name as 'interoperability and portability'. Clarity around this terminology is fundamental. It is key to point out that the following terms are distinct and not synonymous:

- **Interoperability** means the ability of two systems to talk to one another, to exchange messages and information in a way that both can understand, described in the following as interoperability on the PKI level, which means interoperability between PKI systems.
- **Data portability** means the ability to move data (files, documents, database tables, etc.) from one system to another, and have that data usable in the other system.
- **Application portability** means the ability to move executable software from one system to another and be able to run it correctly in the destination system.
- **Accessibility** means the non-discriminator ability to access the relevant information without obstacles or protocols which block the portability of data.

***Interoperability on PKI level:***

When the connector of an ISO15118-2 EV is plugged into an ISO15118-2 charging station (CS), the CS will present its "Supply Equipment Charging Controller – SECC – certificate" for initiating the so-called Transport Layer Security – TLS - Handshake by the EV. In order, for the EV to accept the CS, it is necessary that the SECC-Certificate is trusted by the EV. This means the EV has in its "TrustStore" the RootCA (Root Certificate Authority) of the SECC certificate. The TrustStore is defined in this example as a list of RootCAs, which are accepted/trusted by the EV. The EVs must have in their TrustStore (i.e., must trust) all the SECC RootCAs (i.e. all the V2GRootCAs)

Here the topic is "Interoperability" on a PKI level: In addition to a user interface in the vehicle that enables the user to confirm whether they trust the certificate, the ability to cooperate is based on communication within the PKI ecosystem.

***Interoperability on Data level:***

When an EV-driver wants to activate its EMSP subscription on its EV, it will ask its EMSP to generate the "Contract Certificate" (i.e. the authentication token the EV will use for each charging session managed in a Plug & Charge mode). The EMSP must have the ability to generate this certificate.

But this Certificate will be active/useful, only if it is installed in the EV. There are three main paths to do so:

1) EMSP will transmit this certificate to the EV-OEM, which will push it to the EV for installation .

or

2) EMSP will transmit this certificate to CSO, which will transmit it to the charging station which will transmit it to the EV for installation.

or

3) EMSP will install the certificate via the in-vehicle interface which will be enabled by the EV User/Owner PIN.

In each situation, the EMSP must be able to collaborate with EV-OEM-systems and with CSO-systems. Here the topic is on Data Portability: The ability to cooperate is based on data exchange.

***Interoperability on governance level:***

Apart from the above-described technical level of interoperability, there is also a *governance level interoperability.* Governance describes in this case the concept of operating a PKI for supporting Plug & Charge, including a clear specific description of the IT system for Plug & Charge (which are normally the CSMS backend system to operate charging stations, the eMSP backend system to manage EV users, the EV-OEM backend system as well as the Plug &Charge ecosystem to manage the exchange and encryption of certificates between these backend systems), as well as the organizational structure of the Plug & Charge PKI Service provider. It also details how security and reliability of operating this system are to be ensured. This is normally published in the so-called certificate policy (CS), which needs to be published by every PKI Provider, based on the general requirements of operating a PKI.

In a competitive market, service providers, who are offering a similar service, need to decide how they are competing – this can be based on pricing, quality, and or service differentiation. This is the desired direction to ensure, that customers can select their service providers based on their own interests and business models. Nevertheless, to enable interoperability of the different service providers, it needs to be ensured that all parties are relying on a similar (minimum) level of requirements, IT Security, etc..

This can be ensured by publishing similar mandatory requirements, which need to be fulfilled by all service providers. This can range from a similar requirement to fulfill specific security audits like ISO27001 or similar, and can also include a neutral certification program by the European Union itself that will allow a PKI service provider to start a business model based on ISO15118-2/-20

**Recommendation**

Members of the STF Sub-group on Governance & Standards suggest the European Commission (DG MOVE) to **ensure interoperability between PKIs (PKI systems) in the EU**. This should be achived with the relevant provisions in a delegated/implementing act under AFIR (e.g., by setting guidelines concerning governance rules for PKIs)

## 1.2. The standardization gap in the PKI ecosystem for Plug & Charge

**Context:**

For understanding the PKI ecosystem, three fundamentally different topics have to be taken into account: ISO15118, Public Key Infrastructure (PKI) and "Plug & Charge (PnC)":

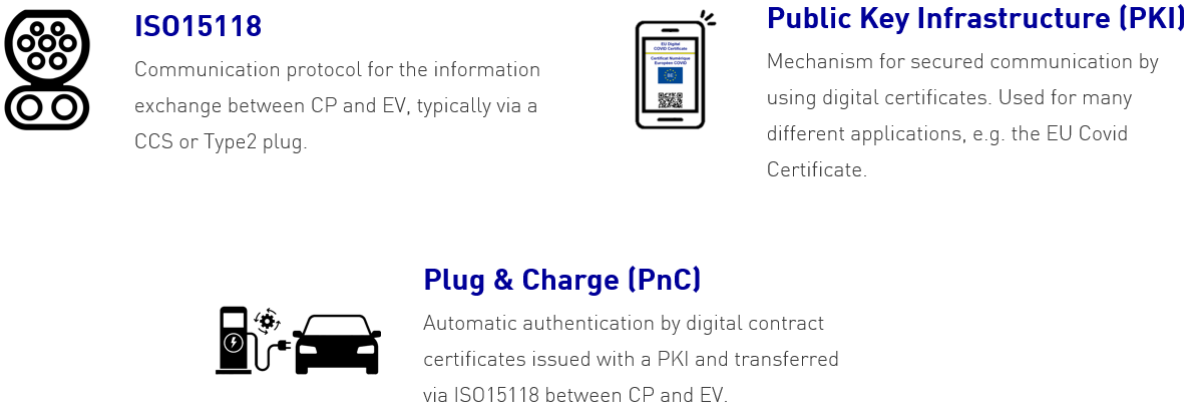


**Figure 12:** Overview about the roles in a Plug & Charge environment

**ISO 15118** is a communication protocol between electric vehicle (EV) and charging station (CS). Conventional AC or DC charging via CCS or Type2 plug works by both systems (EV and CS) exchanging the necessary data such as charging voltage or current. Apart from purely physical parameters, also digital certificates can be exchanged if the parties have access to the relevant Public Key Infrastructure (PKI).

**A Public Key Infrastructure (PKI)** is generally used to enable secure communication by encrypting or signing information with digital certificates. A known application at European level, backed-up by EU legislation, is the EU Digital Covid Certificate[22]. Since the standard ISO 15118 enables the exchange of certificates between EV and CS, a PKI can also be used to secure their communication. However, ISO 15118 is merely the transfer mechanism for certificates both EV and CS have been issued via their backends by the PKI. Related processes to the PKI, e.g. issuing of certificates, is covered by PKI-related services within a PKI ecosystem.

A driver can use automatic authentication via **Plug & Charge (P&C)** if both CS and EV have valid certificates from the PKI and are able to communicate those certificates with each other by ISO 15118.

For a working Plug & Charge environment, the different market roles of Charging Station Operator (CSO), E-Mobility Service Provider (EMSP), Vehicle Manufacturer (EV-OEM), and Public Key Infrastructure (PKI) need standardized communication and processes. Some

[22] https://commission.europa.eu/strategy-and-policy/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en

parts of the ecosystem are standardized whereas there are still gaps. The overview of the ecosystem standardization and the identified gaps are visualized below:

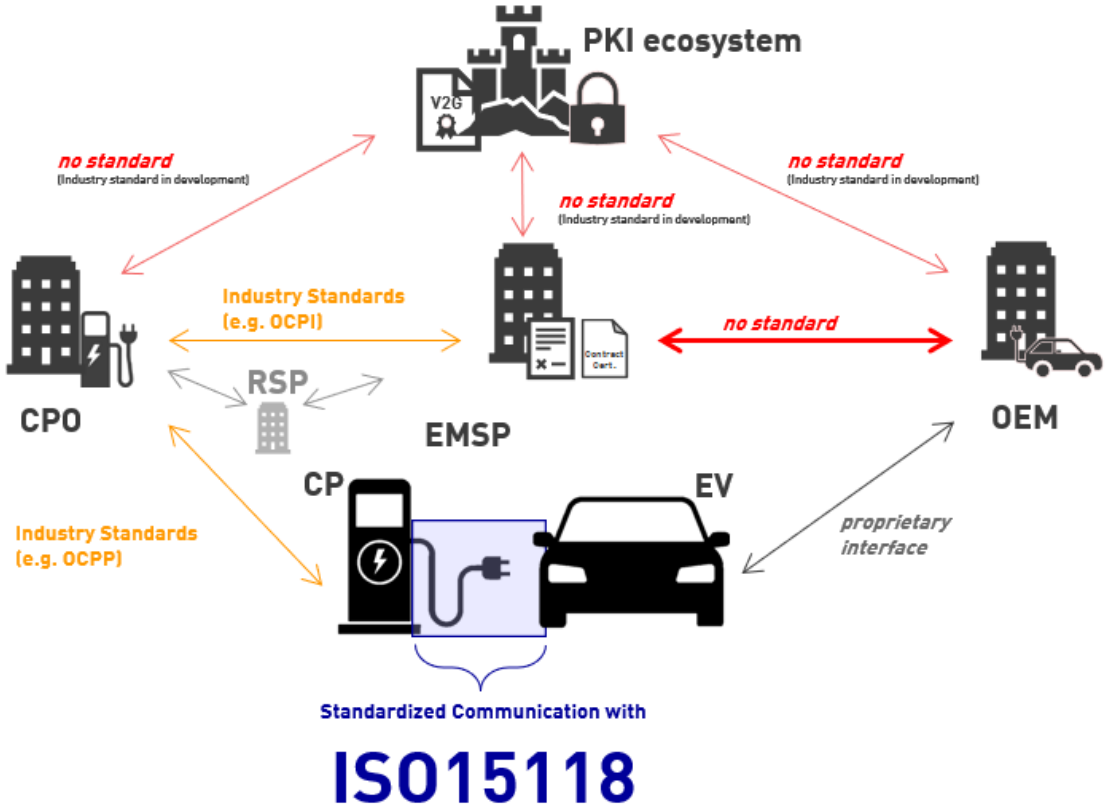


**Figure 13:** Communication protocols in the E-Mobility ecosystem. The scope of the standard ISO 15118 is depicted in blue. Note: Behind each role can be multiple entities (multiple CSOs, EV-OEMs, PKI ecosystems etc.)

The industry initiated the development of the "Open Plug & Charge Protocol (OPNC)" which aims at publishing the first version of the protocol by the end of 2023. The goal of OPNC is to become the industry standard for communication in the PKI ecosystem (see note "industry standard in development" above). The work on OPNC has started in March of 2023 and will be facilitated by CharIN.

In addition to the existing absence of communication standards to complete the whole ecosystem, there are a significant number of non-standardized processes in the ecosystem, e.g.:

- Access of the EV driver to the provisioning certificate identifier (PCID) and the process to transfer it to the EMSP. Every EV-OEM has a different solution.
- Definition of a PCID in ISO 15118-2.
- Installation process of contract certificate in the EV ("multi-contract handling")
- Status information about the contract certificate for the EMSP (e.g., "ready to install", "installed and active", "deactivated", "queued")
- Handling of expired certificates.
- Interoperability mechanism between multiple PKIs.

Obviously, an ecosystem with non-standardized processes as well as non-standardized communication paths must be further developed. This is being done in multiple expert groups (e.g., CharIN PKI Task Force, Mobena project group, OPNC committee, etc.)

**Recommendation**

Members of the STF Sub-group on Governance & Standards suggest the European Commission (DG MOVE) to **support the development process of the needed communication standards and protocols**. In this respect, members recommend that that individual features should not be picked out of a standard in order to mandate them. In consequence, Plug & Charge as a feature should not be mandated.

## 1.3. Ensuring a working Plug & Charge environment: User access to the PCID

**Context:**
In general, for a non-discriminatory PnC feature, all EVs shall support contract certificate installation independent from which EMSP is selected by the customer. The first step in the ability to install a contract certificate for the user is to obtain the PCID of the respective vehicle.

Therefore, there shall be an easy way for a user to take possession of PCID. For example, this can be provided via common digital interfaces for data exchange, where the user is able to extract the data in an easy and convenient manner from those means to provide the information further to the EMSP, for instance by means of an in-vehicle interface.

To achieve this, **the user should be able to obtain the PCID as a human (string) and computer readable (QR) code from an easily accessible HMI (EV, App, etc.)**. In addition, if available, an authentication framework with automated data exchange of PCID to the desired EMSP shall be provided.

It is important to note that this would be indispensable to fully enable a EV user to install a contract certificate via the EMSP app. By scanning the PCID via a QR code, it is transferred to the EMSP. Subsequently, the EMSP can trigger the contract installation via the relevant PKI system through the EV-OEM or the EVSE which in the end is to be executed by the EV-OEM in the EV. Making the PCID complicated or just non-accessible for end users would prevent non-discriminatory installation paths for independent EMSPs.

In addition, an EV-OEM should define security measures to protect the EV from misuse of the PCID like unintentional installation of contract certificates.

**Recommendation**

Members of the STF Sub-group on Governance & Standards recommend the European Commission (DG MOVE and DG GROW) to **ensure by the necessary EU legal means that the user can obtain the Provisioning Certificate ID (PCID) as a human (string) and computer readable (QR) code from an easily accessible Human Machine Interface (HMI)** (e.g., EV app, etc.). The current access to the PCID depends on EV-OEMs, being different in every case, thus, harmonisation is required.

In addition, if possible, an authentication framework with automated data exchange of PCID to the desired EMSP shall be provided. For example, this would enable a end user to install a contract certificate directly via the EMSP app. By scanning the PCID via a QR code it is transferred to the EMSP. Subsequently, the EMSP can trigger the contract installation via the relevant PKI system (which is part of the EU PKI ecosystem) through the EV-OEM or the EVSE which in the end is to be executed by the EV-OEM in the EV. Making the PCID complicated or just non-accessible for end users would prevent non-discriminatory installation paths for independent EMSPs.

## 1.4. Non-discriminatory Contract handling for Plug & Charge based on ISO 15118

**Context:**

If an EV supports ISO 15118 Plug & Charge, the handling, namely the installation, update, removal and prioritization of EMSP contracts in the EV needs to be defined. This situation requires the application of relevant legislation to ensure the user has full control over his EMSP contracts and is able to easily install, remove, update and prioritize contracts as he/she wishes.

To put the user in control, EV-OEMs whose vehicles support ISO 15118 Plug and Charge shall allow any EMSP to easily install, deinstall and prioritize their preferred contract(s) in a non-discriminatory way. This includes an equal level of technical complexity of installation and revocation processes, but also the display and visibility of EMSP contracts.

**Recommendation**

Members of the STF Sub-group on Governance & Standards suggest the European Commission (DG MOVE and DG GROW) that in order to **enable the non-discriminatory installation of contract certificates in the near term**, by obliging EV-OEMs through relevant EU law to:

1) Publish the necessary information on how EMSPs can obtain the Provisioning Certificate ID (PCID).
2) Publish the necessary information on how EMSPs can provide Contract Certificates (CC) to be installed into the electric vehicle.

Members of the STF Sub-group recommend that these requirements are included in the governance rules and onboarding guidelines for PKI systems under the future EU PKI ecosystem. Moreover, these requirements shall be included in the applicable legal instruments for electric vehicles, including a revision of EU type approval.

Further, it is recommended that DG GROW and DG MOVE collaborate with their relevant leiglstiave instruments to introduce the above stated requirements into applicable legal instruments, not only for infrastructur (AFIR) but also for vehicles (type approval).

## 1.5. Anti-competitive behaviour in Plug & Charge: Self-preferencing of EMSPs

**Context:**

In existing and future implementations of Plug & Charge, **potential anti-competitive behavior towards third-party EMSPs can be seen in terms of the in-vehicle user experience**, visibility and technical complexity due to the dominant position of the EV-OEM. One example of such behavior already in the market is that **a number of EVs in the market only accept contract certificates of one specific EMSP,** namely the OEM-owned EMSP.

EV-OEM-owned EMSPs are in competition with third-party EMSPs in the e-mobility market. Due to the business interest between EV-OEM and EV-OEM-owned EMSPs, there is a growing risk for anti-competitive behavior in the e-mobility ecosystem. Further examples of potential anti-competitive behavior are:

- Direct access for EV-OEM-owned EMSPs to Plug & Charge contract installation in the EV whereas other EMSPs must go through a more complicated installation process
- Pre-installed Plug & Charge contracts of the EV-OEM-owned EMSP upon vehicle delivery without options for users to set a preferred Plug & Charge contract or overrule default contract
- More prominent visualization of EV-OEM-owned EMSP certificates in the selection screen without options for users to change (visualization) preferences

Other examples of anti-competitive behavior – which are currently not happening in the market – could occur in the relationships between CSO and CSO-owned EMSP, RSP and EMSPs as well as other market roles.

European Law addresses abuse by one or more undertakings of a dominant position in Article 102 TFEU (ex. Article 82 TEC) and the specifying document "Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (2009/C 45/02)". Whilst the Guidance is from 2009 and has been applied in investigations towards, for example, Amazon, Microsoft and Google, recent case law indicates that updates are necessary.

For example, in June 2017, the EC found that Google's more favorable positioning and display, in its general search results pages, of its own comparison-shopping service compared to competing comparison-shopping services infringes article 102 TFEU. In 2021, the General Court confirmed, for the first time, that **self-preferencing by a dominant company may amount to an abuse of article 102 TFEU**. "Self-preferencing" is the situation where a vertically integrated dominant company uses its own asset, such as its platform, to favor the positioning or sale of its own goods or services at the expense of rivals.

**Recommendation**

Members of the STF Sub-group on Governance & Standards suggest the European Commission (DG MOVE and DG COMP) to **ensure that apropriate EU regulation and governance rules provide a level playing field between EMSPs, and with other market actors**, so that every EMSP (third-party or EV-OEM or CSO owned) can provide to end users services based on equal, seamless (in-vehicle) user experience and functionalities for Plug & Charge and no "self-preferencing" occurs.

Members of the STF Sub-group recommend that DG MOVE and DG COMP jointly address the risk highlighted and assess whether such behavior is already unlawful or penalised through existing regulation before the market uptake of Plug & Charge.

## 1.6. Data Sensitivity with Plug & Charge EMSP contracts in EVs

**Context:**

For the PnC functionality, supported by a Public Key Infrastructure (PKI), contract certificates will be generated and issued by EMSPs. Those contract certificates need to be installed in the EV. This creates a new situation: The EV-OEM can know the EMSP contract of the user. Since the EV-OEM has also complete insight into the charging behavior of the user (e.g., energy charged publicly and at home), the information about which EMSP contract the user has can be critical. This is especially true in case an EV-OEM also has an affiliated EMSP (i.e., which most EV-OEMs nowadays have). Then sensible information about direct competitors of the affiliated EMSP are available to the EV-OEM. If used, this creates an unfair disadvantage to EMSPs not affiliated with an EV-OEM.

An analogy from the energy market would be if the energy supplier had access to the contracts and consumption data of the house grid connections at the in-house grid network operator. Since the normal data protection and anti-trust laws fall short, there is unbundling in the energy sector.

Because both EV-OEMs and CSOs have a primary role in the handling of contract certificates to make them available for installation in the EV, both parties are in the

position to gain additional data insights, based on the reconstruction of charging, and therefore user behavior. However, the quality of data and the level of insight into user behavior is different for an EV-OEM compared to a CSO. Therefore, the situation in the PnC ecosystem should be addressed.

**Recommendation**

Members of the STF Sub-group on Governance & Standards suggest the European Commission (DG MOVE) to **introduce a topic for the 2023/2024 working programme of the STF sub-group on data sensitivity in the Plug & Charge ecosystem**. Members suggest the following tasks to include for discussion:

1. Define and evaluate technical and legal solutions to ensure same level playing field for all ESMPs (i.e., market role definition);
2. Identify option(s) to eliminate additional data insights on installed Contract Certificates (i.e., anonymization of contract information)

# 2. ISO 15118 – User access to functionality and smart charging

## 2.1. User access to features and functionalities of ISO 15118

**Context:**

The standard ISO 15118 in its versions ISO 15118-2 and ISO 15118-20, defines several functionalities and features in the e-mobility environment and its required communication parameters between CS and EV. The mandatory elements of the features & functionalities within the standard are implemented in EVSE and EV and for some of them, no user interaction is necessary, e.g. for a TLS handshake.
However, for some of these features there is additional user interaction needed to make them available and accessible to the user. The means for this user interaction shall be implemented by the respective entities to follow the mandate of the standard and enable users to benefit from them at their will. The question of end user accessibility is not covered by the standard ISO 15118 as it just defines communication between EV and EVSE on a technical device level (communication controller).

Table 1 aims to provide an overview of the **capabilities of both ISO 15118-2 and -20 protocol**. The table also highlights necessary user interaction categories and the required user interface to control the respective protocol capability. In the table the generally known functionalities of ISO 15118 are listed, including the required action from a user perspective (User Interaction) and the elements needed to enable the user interaction (User Control Interface Elements).

**Table 1.** Overview of Functionalities and Capabilities of ISO 15118

| Functionality | Feature | User Interaction | User Control Interface Elements | ISO15118 -2 | ISO15118 -20 |
|---|---|---|---|---|---|
| AC charging | Basic charging | Configure | Set preferences for time, power/energy, and cost (Schedule) | X | X |
| DC charging | Basic charging | Configure | Set preferences for time, power/energy, and cost (Schedule) | X | X |
| Bidirectional Power Transfer | Charging / Discharging capabilities | Enable/disable | On/Off Switch, max discharge power, preferred safety SoC range of vehicle battery/user | | X |
| | | configure | | | |
| Automated Connection Device | Automated conductive charging | Enable/disable | On/Off Switch | | X |
| Wireless Power Transfer | Contactless charging | Enable/disable | On/Off Switch | | X |
| Security | TLS encryption for Authorization | N/A | N/A | X | X |
| | TLS encryption for all communication | N/A | N/A | | X |
| | Authentication of EVSE | N/A | N/A | X | |
| | Mutual authentication of EV and EVSE | N/A | N/A | | X |
| Plug and Charge (PnC) | PnC Certificate based authorization | Enable/disable | On/Off Switch | X | X |
| | Contract certificate installation via EVSE | N/A | N/A | X | X |
| | PnC multiple Contract Certificate handling | Configure | Prioritization of contracts, installation, deinstall contracts | | X |
| Smart Charging | Charge scheduling on Power and cost | N/A | N/A | X | X |
| | EV Charging Profile ([1] Maximum power demand; [2] Real power demand ) | N/A | N/A | X[1] | X[2] |
| | Optimization of Charging power levels | N/A | N/A | | X |
| | Dynamic charging | Enable/disable and configure | On/Off Switch | | X |
| | | | Departure Time, Target SoC, Min SoC, | | |
| | Provide mobility needs (e.g. Target SoC) via the EVSE | Yes Enable/disable and configure | Switch | | X |
| | | | Departure Time, Target-SoC, Min-SoC | | |
| Renegotiation of charging parameters | with interruption of energy flow | N/A | | X | |
| | with parallel energy flow | N/A | N/A | | X |
| | Change of charging Mode/service | Configure | Switch (scheduled charging to dynamic charging and/ or regular to bidirectional charging) | | X |
| Sleep Modes | Pausing | N/A | N/A | X | X |

| | | | | | |
|---|---|---|---|---|---|
| | Standby | N/A | N/A | | X |
| Pricing information | Indicative cost of energy | N/A | N/A | X | X |
| | Currency-based prices for energy and related services | Inform | Prices, service, (e.g. energy, parking) tax, Fees | | X |

An example for necessary user interaction is the 'Dynamic Charging' mode. To enable this feature the end user first will need to activate/select it via the HMI in order for the EV to pick this charging mode out of a selection of services offered by the EVSE on the ISO15118 protocol level. Secondly, the user will then have to provide his preferences for using this charging mode, like when he plans to leave (Departure Time), and what amount of energy he expects to be in the EV battery ideally (Target SoC), or at minimum (Min SoC).

It is not expected that the user will directly provide his input in terms of energy values in kWh but rather in terms of an expected driving range that the EV then will convert into a corresponding amount of energy (SoC) needed. However, in the context of accessibility it is only important, that the user will have the respective means to provide the necessary input. The detailing of the user interface, like in what format and design this is provided to the user is beyond the scope of accessibility and should be left to the individual EV-OEM.

Another example is the handling of contract certificates for "Plug & Charge". An EV-OEM can implement the Plug & Charge capabilities on a communication level by ISO 15118. However, if no respective interface is provided to the user, the functionality itself is not accessible to the full extent or not at all.

By the definition, in the ISO 15118 standard the EV is the device holding the Plug & Charge enabled EMSP contracts (contract certificates) on behalf of the user. To provide the user with the necessary means to control and manage his contract certificates, the EV does need to provide a user interface for installation and de-installation, as well as prioritization of the user's contract certificates.

Another example would be bidirectional charging. Apart from the implementation on a communication level according to ISO 15118, there must be a user interface where the driver can select whether bidirectional charging shall be activated or not and further also be able to configure according to his needs and preferences (e.g., what energy he is willing to provide from his EV battery) – otherwise the functionality is not accessible.

Both these examples show, without the EV presenting the right level of information and providing the respective control means, that the ISO 15118 capabilities cannot be independently utilized and controlled by the end user.

**For some of the features and functionalities in ISO 15118, there are optional elements and parameters**. Their implementor, if not subject to legal provisions, can decide whether a feature or functionality will be accessible and available as a service to the user. In this context, transparency to end users and B2B partners shall be given. This means general, easily understandable information about what features and functionalities are offered and accessible (e.g., a list of them on a website). On the other hand, this also implies the need to have the proper B2B exchange of information between partners implementing the counterpart of the communication (e.g., which PKI a party is connected to).

**Recommendation**

Members of the STF Sub-group on Governance & Standards suggest the European Commission (DG MOVE) to **ensure the full utilization of the features and functionalities enabled for e-mobility by the standard ISO 15118**. To achieve that, the members specifically recommend the following:

In addition to the requirements on the communication protocol (i.e., ISO 15118) mandate into the applicable legal instruments (i.e., AFIR and type approval) for charging infrastructure and EVs, it is recommended that **DG GROW and DG MOVE collaborate with their relevant legilstiave instruments to ensure the minimum user control elements (as described in Table 1) are provided to the end user via the Human Machine Interface (HMI) in the EV (e.g., in car display or EOBD interface).**

Since there are often misunderstandings when discussing 'features' and 'functionalities' of the ISO 15118 standard, members recommend using the nomenclature for functionalities and features introduced in Table 1. Thereby, all actors can have a unified language and understanding.

## 2.2. Smart charging and the implications of different versions of ISO 15118

**Context:**

Smart Charging (V1G) capabilities are currently introduced and implemented in the market in various forms. When discussing smart charging, even on a European and national legislative level, the concepts and interpretations are not the same. This lack of clarity leads to uncertain definitions and requirements. According to members of the STF sub-group on Governance and Standards, in the latest version of AFIR (March 2023) "smart charging" and its relation to "bidirectional charging" is not adequately captured. Quoting the smart and bidirectional charging definition of AFIR:

- *"smart recharging" means a recharging operation in which the intensity of electricity delivered to the battery is adjusted in real-time, based on information received through electronic communication;"*
- *"bi-directional recharging" means a smart recharging operation where the direction of the electricity flow may be reversed, allowing that electricity flows from the battery to the recharging point it is connected to;"*

Together with the provision in AFIR that "operators of recharging points shall ensure that all publicly accessible normal power recharging points operated by them are capable of smart recharging", this situation creates a difficult interpretation for the market. The reason is that with the above definitions and provisions, one could understand that *bidirectional charging is part of smart charging* and, thus, derive a mandate for bidirectional charging at public charging stations. However, CSOs are not technically able to fulfill this requirement today. Therefore, members of the sub-group propose an improved definition.

A common minimum understanding is that "smart charging" aims at balancing grid constraints and end user mobility needs by enabling a flexible energy transfer. This can be executed according to the following definitions:

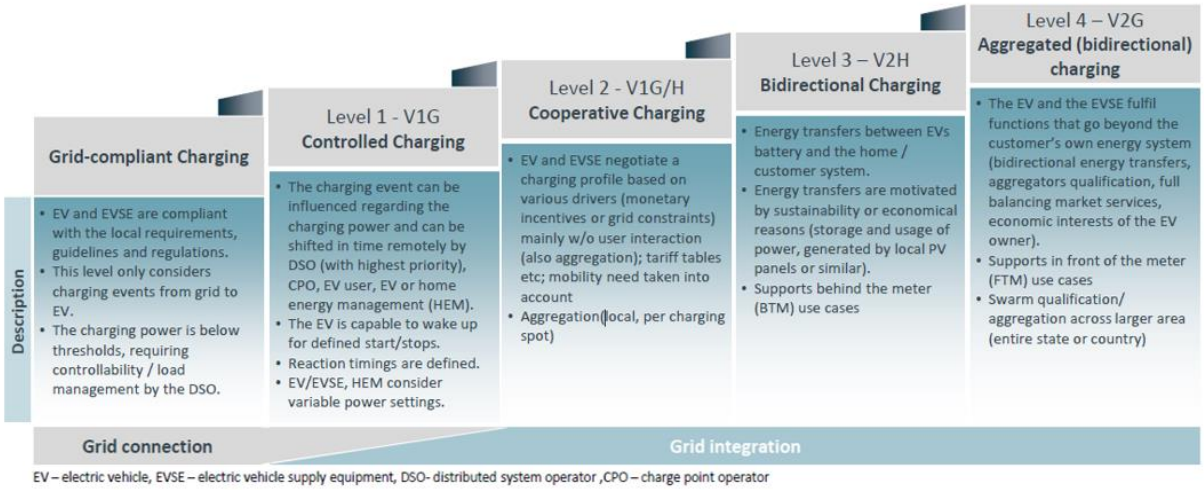


**Figure 14.** Levels of Smart charging based on CharIN

The smart charging concept defined in ISO 15118-2 is very limited, because EVs do not provide a charging profile. They only provide a potential maximum power demand over time, but are not forced to comply with these power requests. Differently, charging stations are obliged to reserve that maximum power requested by the EV for every point in time although it might not be used. An illustration is shown in Figure 15.

Therefore, no effective power/energy management balancing between grid constraints and end-user mobility needs is possible, as vehicles request more (higher) power than they are actually will be using. Further, the defined schedule mechanism would make physically installed EVSEs at e.g. a grid constrained location unavailable to users and this will be limiting utilization and, hence, impacting the real term availablity of infrastructure. The resulting smart charging functionality is not efficient, not scalable for the mass market adoption and moreover, will not support already existing market needs.

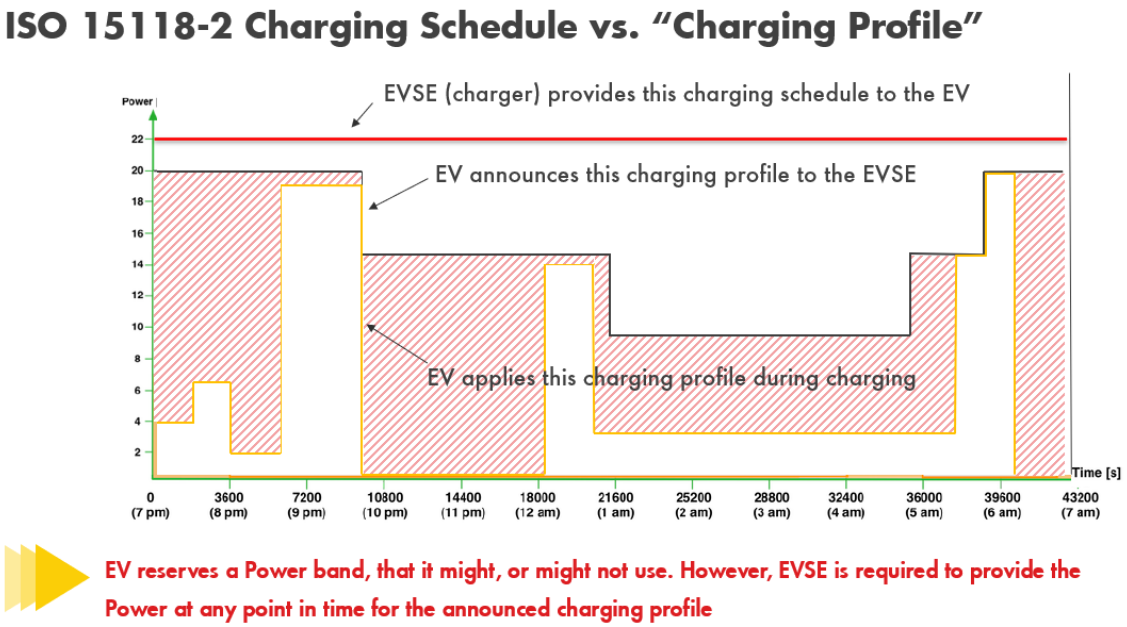


**Figure 15.** Schedule mechanism in ISO 15118-2

With the defined mechanism in ISO 15118-2 the capability for advanced energy transfer (e.g., highly dynamic power adjustment while charging) can only be carried out in an uncoordinated manner between the EV and the EVSE which prevents effective smart charging mechanisms that would allow large scale grid cooperative charging.

The EV is in sole control to authorize a renegotiation (change) request form the infrastructure on an previously agreed charge schedule. This means in order to fulfill changing grid needs the EVSE is depending on the EV to accept its request, even though the EV has no insight into the demand and priority on the grid side. This further deteriorates the ability of the DSOs/CSOs for advanced energy management, or to react to changing grid or local demand conditions in a coordinated manner

In addition to the above limitations, **bidirectional capabilities are not supported by ISO 15118-2,** which are needed for any feature within the domain of V2G(rid), V2H(ome), V2L(oad). However, it is expected that bidirectional capabilities will become more and more important and will trigger further market mechanisms (e.g., energy market participation, congestion, grid balancing). To support future flexibility energy market mechanisms, regulatory authorities and DSOs need to work together on a common approach to set the framework for bidirectional smart charging capabilities. **For this ISO 15118-20 is key**, as it introduces essential extended technical capabilities that are essential for grid support and enable bidirectional charging.

**Recommendation**

Members of the STF Sub-group on Governance & Standards recommend the European Commission (DG MOVE) the following aspects:

1) If smart charging functionalities are mandated, e.g. within AFIR, it should come with a proper definition based on the above introduced levels.
2) If smart charging functionalities are mandated, e.g. within AFIR, this should mean a mandate for ISO 15118-20 as way forward to enable the full extent of smart Charging and support V2G mechanisms in broad perspective. A mandate for ISO 15118-2 will impose critical limits to smart charging in the future.
3) Assign an expert group (e.g. “Activity 3” of STF SG1) also including experts from DG ENER to work out specific recommendations and requirements to address limitations on smart charging. Moreover, the ecosystem needs must be matched with provided protocol capabilities based on the mandated version of ISO 15118.

# 3. Data sharing

## 3.1. User access to data exchange in the e-mobility ecosystem

**Context:**

EV and CS data sharing is essential to enable charging and mobility services (e.g., smart charging capabilities, Vehicle-2-Grid services, value-added services such as EV routing and preconditioning).

As previously introduced, data types (i.e., State-of-Charge - SoC, battery state of health, charging power, etc.) shared between EV and CS are defined by ISO 15118. However, for some use cases, the definitions are incomplete and for some even non-existent. Therefore, there should be a detailed understanding about additional data points within the e-mobility ecosystem and possible additional use cases to ISO 15118 (i.e. bidirectional power transfer, dynamic smart charging, etc.).

Examples for use cases with the need to discuss data sharing between various actors:

- **EV battery Information (e.g. SoC):**
  - Transfer of SoC is optional within ISO 15118 standard, therefore SoC interpretation is dependent on EV-OEM specific implementations This means that SoC definition will differ between vehicles
  - Definition of which SoC to use, or to calculate does not exist, and is not communicated to the User in a uniform way. Therefore, even within the vehicles transferring the value, the meaning will differ for EV driver and other stakeholders
  - Therefore, SoC related functionalities on infrastructure side will differ: SoC visualizations on MSP/CSO side, SoC-based messaging in case of heavy site usage, error analysis capabilities.

- **Preconditioning of batteries prior to fast charging:**
  - The mechanism is not defined and therefore not uniformly deployed. Non-discriminatory functionalities by triggering preconditioning of vehicle batteries could be potentially a solution to optimize charging sessions If implemented, navigation features are likely to be part of EV-OEMs offering only and therefore discriminatory. Therefore, examples of discriminatory implementations are on the market where the EV-OEM navigation system influences charging power of charging stations.
- **Smart Charging (V1G) and bidirectional power transfer (V2G):**
  - To enable energy services with more advanced levels of smart charging and bidirectional functions (see also section **Error! Reference source not found.**), information shared between CS and EV according to ISO15118 do not contain actual energy demands (i.e. required energy till target SoC, available energy till minimum SoC, Energy until maximum SoC. Information about grid constraints by DSOs or tariffs from EMSPs are necessary as well, the exchange of this information is not clearly defined.
- **Charging Station Reservation:**
  - In order to reserve a charging station, a scalable solution for data exchange is necessary prior to the charging event
  - This could even include exchanging information about charge park usage to efficiently route users to free charging stations, especially in peak events such as holidays.

Looking forward, it seems logical to assign the design of the topic “data exchange with EV” to the STF Sub-group on Data. This sub-group is currently working on the data architecture for alternative fuels, including the definition of concrete aspects about e-mobility data types to be made available to the National Access Points (NAPs) of Member States in line with AFIR Art. 20. For this purpose, the STF Sub-group on Data is elaborating two activities and further a collaboration with the NAPCORE group has been defined.

However, to better pool existing expertise on EVs and standards, this discussion should lead to one joint working program between STF Governance & Standards (SG1) and STF Sub-group on Data (SG2) to work on the architecture and design of the data elements that will be shared and how data should be exchanged between the parties within the e-mobility ecosystem. This joint working program should also involve experts of the D4E expert group from DG ENER. The Commission will have to define a joint work program for D4E and the STF on Data by end 2023. Finally, cooperation and sharing of information with relevant expert group under EU vehicle type approval is also recommended.

**Recommendation**

Members of the STF Sub-group on Governance & Standards recommend the European Commission (DG MOVE) to **define a new activity within the STF Sub-group on Governance & Standards, and Data working programme 2023/2024 to take address the architecture and design of the "data exchange with EV"**.

Procedurally, for the in-vehicle data work to succeed, solid cooperation and synch should be established between the different Commission services (DG MOVE, DG GROW and DG ENER), expert groups and industry fora. Content-wise, members suggest the following tasks to include for discussion in the new activity of the STF Sub-group on Governance & Standards, and Data working programme 2023/2024:

1) Assess all current legislative actions in the field of data exchange (notably RED2, EU Data Act, and the initiative on access to in-vehicle data act)
2) Define all required data points and use cases, both mandatory and optional.
3) Identify all data attributes and types for the data exchange within the e-mobility ecosystem.
4) Propose a uniform way to regulate the in-vehicle-data list in sync with all initiatives and legal actions (i.e., AFIR, type approval, etc.)

## 3.2. Unique electric vehicle identifier for fraud detection and grid integration

**Context:**

Devices connecting to EV charging infrastructure need to be traceable out of multiple reasons, for example due to detection of fraud and technical problems with individual models. Communication protocols (DIN SPEC 70121, ISO15118-2 and ISO15118-20) specify an identifier called electric vehicle communication controller ID (EVCCID). This EVCCID is transferred in all cases and, thus, it must be directly applicable for traceability. There is no alternative identifier which is available in all communication protocols and with all authentication types.

For **fraud detection**, such an identifier can be used in investigating malicious behavior at charging sites. Most charging sites are operated without video surveillance or personnel on site therefore a device identifier is the only way to gain intelligence about fraudulent activities.

For **error identification**, such an identifier can be used to find products causing problems in the charging process. For example, if an EV model is updated remotely and creates issues in the charging infrastructure, the problematic model can quickly be identified, and the error can be handled accordingly. This becomes even more important with the further ramp up of electric vehicles, the increasing needs for grid integration (not limited to bi-directional charging) and the following influence on the stability of the power grid.

For **offline charging**, such an identifier can be used to determine availability. For example, if a charger is offline then users with a trackable identifier could be allowed to charge whereas without such an identifier the authentication will be rejected because of fraud prevention.

In DIN SPEC 70121 and ISO15118-2, the EVCCID is defined as being equivalent to the MAC-Address of the controller. In ISO15118-20, a more distinct definition of the EVCCID is given. The only addition required for legislation is the stability of the EVCCID over lifetime of the controller, i.e. the EVCCID will only change if the controller itself is being changed. EVCCID-spoofing, which is already happening in the market, should be prevented as it opens a potential attack vector to critical infrastructure.

A unique EVCCID that is stable over lifetime is *GDPR-relevant*. Although the EVCCID does not track a person but a device, it is linkable to a vehicle and thus also to a person if additional information is acquired. It is thus comparable to a VIN which is visible in the windshield of vehicles. In theory, a CSO could try to track individuals using the EVCCID. However, since users of public charging stations must pay for energy, a more direct tracking method is offered by the payment method (EMAID, credit card number, etc.). Therefore, the EVCCID will not offer additional possibilities concerning user anonymity. In opposition, using device IDs for fraud detection is allowed under GDPR:

*"The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned."*[23]

However, users could prefer not to share a device identifier for privacy reasons. This preference could be integrated similarly to the MAC-address randomization in mobile phones. There, the user has the choice to set for a stable or a randomized MAC-address in the device and accept certain feature limitations. This enables the user to control whether privacy or feature accessibility is valued higher. This concept could be transferred to the e-mobility industry.

[23] See Recital 47 of the GDPR from April 27th, 2016: https://gdpr-info.eu/recitals/no-47/

**Recommendation**

Members of the STF Sub-group on Governance & Standards recommend the European Commission (DG MOVE) that **the already existing electric vehicle communication controller ID (EVCCID) can be used as an identifier for fraud and error detection**. Thereby it is suggested:

1) The EVCCID transferred by the electric vehicles follows the definitions of the respective standard (DIN SPEC 70121, ISO 15118-2 or ISO 15118-20), depending on the EV implementation.
2) EV-OEMs ensure the EVCCID remains unique and stable over lifetime.
3) EV-OEMs integrate a randomization functionality for EV users. With this functionality, users shall have the choice and the means to share a stable, unique EVCCID or to randomize it and accept fewer functionalities (e.g., no offline-charging, no bidirectional charging – depending on the CSO security policy). If the user sets a randomization mechanism for the EVCCID, then the EVCCID shall indicate this randomization similar to the concept already established in modern mobile phones.

Further, it is recommended that **DG GROW introduces these requirements into applicable EU legal instruments for vehicles (type approval)**.

# 4. Standards, mandates and conformance

## 4.1. Ensuring synchronized requirements between electric vehicles and recharging infrastructure

**Context:**

In Activity 1 of STF Sub-group on Governance & Standards, it was clarified during technical discussion that AFIR can set legally binding requirements on charging infrastructure only. This circumstance has been analyzed and confirmed by DG MOVE during the elaboration of this Activity 2.

The legal basis for AFIR is targeted at charging infrastructure but not at vehicle requirements, which are regulated by DG GROW (e.g., EU vehicle type approval). In consequence, members of the sub-group point out, that only adding requirements on the infrastructure in AFIR risks to lead to a one-sided regulation for the recharging infrastructure, since requirements towards electric vehicles are not - and cannot be - defined there.

As charging communication is based on a bi-directional communication protocol (server/client) the desired level of security and interoperability in the market cannot be reached by only regulating one of the two communication participants.

For example, concerning the communication standard itself: a delegated act under AFIR could mandate e.g. ISO 15118-20:2022 and/or ISO15118-2:2014 for charging infrastructure as of 2026. However, without a parallel legal mandate for electric vehicles, it is absolutely uncertain whether EV-OEMs would apply the same version in the same timeline. Moreover, this situation could worsen even more if a competing standard to ISO

15118 would be introduced in the market. Therefore, parallel legal mandates for electric vehicles and infrastructure are considered indispensable.

At the level of functionalities, this bears the risk for the end user and the ecosystem to be strongly limited by supporting different versions of the same standard, incompatibility of features (e.g. Plug & Charge) or the capabilities for 'smart charging', which will create an abyss between market needs and available capabilities.

The only identified legal instrument where requirements concerning EVs can be defined in Regulation (EU) 2018/858 on the approval and market surveillance of motor vehicles (vehicle type-approval and testing). Moreover, it is also important to consider Over-the-Air-Updates (OTA) for the homologation of vehicles according to UNECE R155[24] (Cybersecurity Management System) and UNECE R156[25] (Software Update Management System).

**Recommendation**

Members of the STF Sub-group on Governance & Standards recommend the European Commission (DG MOVE) to forward the requirements below to DG GROW for inclusion into applicable legal instruments, namely EU vehicle type-approval framework (Regulation (EU) 2018/858 on the approval and market surveillance of motor vehicles).

Technical requirements for electric vehicles shall be parallel to those from recharging infrastructure (AFIR). This approach would ensure a future syncronised communication and supported functionality between EVs and infrastructure in the EU. The following requirements should be taken into account in an upcoming revision EU vehicle type-approval:

- Mandate of communication standards, ISO 15118-20:2022 and/or ISO15118-2:2014 (Reference to Block 3, Section 4.2)
- User availability of the PCID for Plug & Charge (Reference to Block 3, Section 1.3)
- Contract handling transparency for Plug & Charge (Reference to Block 3, Section 1.4)
- Ensuring data privacy in Plug & Charge environment (Reference to Block 3, Section 1.6)
- Accessibility of ISO 15118 features for the end user (Reference to Block 3, Section 2.1)
- Data availability in the specified use cases (Reference to Block 3, Section 3.1)
- Availability of the EVCCID (Reference to Block 3, Section 3.2)

[24] UN Regulation No. 155 (UN R155) is a regulatory framework created by the World Forum for Harmonization of Vehicle Regulations (WP.29), a working party within the Sustainable Transport Division of the United Nations Economic Commission for Europe (UNECE). UN R155 requires the presence of a cybersecurity management system (CSMS) in vehicles. In a nutshell, a CSMS ensures that cybersecurity practices and measures are adequately applied across the development process and life cycle of vehicles.

[25] UN Regulation No. 156 (UN R156). UN R156 requires "Software Update Management System (SUMS)" to implement a systematic approach defining organizational processes and procedures to comply with the requirements for delivery of software updates.

## 4.2. Mandating standards (ISO 15118)

**Context:**

If a standard is mandated in EU legislation, additional aspects should be taken into account; such as the question of when that mandate applies for devices or if related standards are also need to be considered as part of the mandate. Thereby, implementation of standards as e.g. ISO 15118 should be based on the defined level of optionality included in the standard. The standards already define the required level of optional and mandatory implementations for industry, based on their concrete technical features and security requirements. For clarity to all industry members, the following steps are recommended when mandating a standard.

As an example, for a potential ISO15118-20 mandate as minimum specification with wired communication, this would mean at least including the following parts: ISO 15118-20:2022 Ed.1, ISO15118-3:2015 Ed1. For an overview and description of all ISO 15118 parts, see the following table:

| ISO15118 Part | Title | Status |
|---|---|---|
| 1 | General information and use case definition | Ed 2: IS (2019) |
| 2 | Network and application protocol requirements | Ed 1: IS (2014)<br>Ed 2: DIS (2023) |
| 20 | Network and application protocol requirements (with additional functionalities) | Ed 1: IS (2022) |
| 3 | Physical and data link layer requirements | Ed 1: IS (2015) |
| 4 | Network and application protocol conformance test | Ed 1: IS (2018)<br>Ed 2 UD (2023) |
| 5 | Physical and data link layer conformance test | Ed 1: IS (2018) |
| 6 | Physical and data link layer requirements for differential Power Line Communication | UD (2024) |
| 8 | Physical and data link layer requirements for wireless communication | Ed 2: IS (2020) |
| 9 | Physical and data link layer conformance test for wireless communication | Ed 2: IS (2022) |
| 10 | Physical layer and data link layer requirements for wired ethernet communication | UD (2024) |
| 21 | Network and application protocol conformance test - Common | UD (2024) |
| 22 | Network and application protocol conformance test - Security | NS |
| 23 | Network and application protocol conformance test - conductive AC/DC charging | NS |
| 24 | Network and application protocol conformance test - Wireless Power Transfer | NS |
| 25 | Network and application protocol conformance test - Automatic connection device pantograph DC | NS |

IS ≡ International Standard
DIS ≡ Draft International Standard (dates stated are expected publication times)
UD ≡ Under development (dates stated are expected publication times)
NS ≡ Not yet started

**Recommendation**

Members of the STF Sub-group on Governance & Standards recommend the European Commission (DG MOVE) to mandate standards under AFIR by adhering to the following principles:

1. **Mandate a "full" standard**: Any standard mandate in legislation via AFIR and secondary legislation (i.e., delegated acts) should be based exclusively on prescribing the full parts of the standard (e.g., ISO 15118-20:2022 / ISO 15118-2:2014) and should not prescribe a subset or specific functionalities, as this would bear a high risk to negatively affect interoperability. Additionally, mandating full specifications prevents selective implementations in the industry that could also negatively affect interoperability.
2. **Mandate specific versions**: If a standard is to be mandated, the exact version including related/required standards should be prescribed. For example, instead of mandating "ISO 15118" the legislation should state specifically a mandate for "ISO 15118-20:2022" as well as "ISO 15118-1:2019 (use cases) and ISO 15118-3:2015" (physical layer requirements). This means that every device (EV, EVSE) needs to implement the specification that is applicable to the device. For example, a DC EVSE for charging would at least have to implement the feature set for DC charging but does not have to implement the AC features because they don't apply to that device.
3. **Mandate related standards**: A standard series such as ISO 15118 is comprised of multiple parts (see the following list). For example, ISO 15118-1 defines the use cases, ISO 15118-3 & 8 define the physical layer of the communication and ISO 15118-20 defines the communication protocol messages. In order to have interoperability, all relevant parts of the respective standards should be mandated to enable the highest level of interoperability and prevent e.g. a party trying to communicate with the protocol of ISO 15118-20 via an undefined physical layer. For a mandate of a technical standard, it is recommended to list all the required parts to ensure a basic level of functionality and interoperability.
4. **Mandate including a timeline**: If a standard is to be mandated, an implementation timeline should be given. The timeline should reflect a reasonable period for implementation (e.g., 24 months for ISO 15118-20:2022) so that relevant market parties can do the necessary development/implementation activities to comply with the new regulation.
5. **Mandate only for new devices**: When mandating a standard, it should only apply to new devices. For an EVSE device, this means the mandate only applies to new installations. For an EV the mandate will be reflected in the type approval and will only apply to the EVs that will be delivered with the new type approval. No retrofit should be requested for the devices.

## 4.3. Conformance to standards

**Context:**

Conformance is defined as, how well something, such as a product, service or a system, meets a specified standard and may refer more specifically to: Conformance testing, testing to determine whether a product or system meets some specified standard.

Given a mandate of any standard, the question in the industry remains of "how can conformance be ensured and validated" and "how can a player ensure correct implementation following the requirements from a mandate?". Some standards have defined their conformance via a certification process, other standards have defined a set of conformance tests.

**Recommendation**

Members of the STF Sub-group on Governance & Standards recommend the European Commission (DG MOVE) that any mandate for a standard stipulated by EU regulation, require a request for correspondent proof of conformance via certification or audited conformance testing, to ensure implementations are correct, compliant, and interoperable.

The assurance of conformance is to be achieved by a third party certification/auditing program, allowing accredited test organizations to provide independent certification at an established assurance level.

- For ISO 15118-2 the conformance is specified in the ISO 15118-4 document.
- For ISO 15118-20 the conformance is specified in the ISO 15118-21, -22, -23, 24 and -25 documents. These documents are not yet available.

Overall, there is neither for ISO 15118-2 nor for -20 a certification program defined and available. To ensure common conformance, the European Commission should consider in the future having a EU-wide conformance/certification process available and active for all future mandated standards.

## 4.4. Backwards-compatibility for the EVSE-EV Interface

**Context:**

This aspect has been raised in Activity 1 and was to be concluded as part of Activity 2 of the STF Sub-group on Governance and Standards.

**Recommendation**

Members of the STF Sub-group on Governance & Standards recommend the European Commission (DG MOVE) to adopt the following description and definition for backwards compatibility with the ISO 15118 standard.

- Backwards-compatibility for the EVSE-EV Interface: ISO 15118 communication protocol allows two end points to negotiate during an initial handshake phase which version of the ISO 15118 protocol is preferred. The preferred version is supported by both EV and EVSE and they agree to operate under it during the charging process.

  NOTE 1: Such a technical protocol capability can also ensure forward compatibility as well as general feature negotiation.

  NOTE 2: The backwards and forward compatibility capability of a protocol does not automatically result in upgradeability, which describes the concept that all products can always be upgraded to support the latest version of a protocol.

  NOTE 3: In case a common preferred version of the ISO 15118 protocol cannot be identified during the initial handshake a fallback protocol shall be activated to ensure the basic function of vehicle charging.

The fallback protocols are:

- for AC Charging: IEC 61851-1
- for DC CCS-Charging: DIN 70121

  NOTE 4: The fallback protocols defined in NOTE 3 should be conditioned to well defined rules to exchange the fallback protocol. A future upgradeability of the fallback protocols to 15118-20 should be a clearly indicated goal.

## GETTING IN TOUCH WITH THE EU

**In person**

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

**On the phone or by email**

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

– at the following standard number: +32 22999696 or

– by email via: https://europa.eu/european-union/contact_en

## FINDING INFORMATION ABOUT THE EU

**Online**

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

**EU publications**

You can download or order free and priced EU publications at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

**EU law and related documents**

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

**Open data from the EU**

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

MI-07-23-280-EN-N

Publications Office
of the European Union

doi:10.2832/010726
ISBN: 978-92-68-06051-3