European Commission

Support Study on the development of a governance framework for the EU Public Key Infrastructure (PKI) based on the standard ISO 15118

Final Report

July 2023

pwc

EUROPEAN COMMISSION

Directorate-General for Mobility & Transport (DG MOVE)

Directorate B — Investment, Innovative and Sustainable Transport

Unit B4 — Sustainable & Intelligent Transport

Contact: Dr. Saki GERASSIS DAVITE

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

European Commission
B-1049 Brussels

Support Study on the development of a governance framework for the Public Key Infrastructure (PKI) based on the standard ISO 15118

Final Report

2023 Directorate-General for Mobility and Transport (DG MOVE)

LEGAL NOTICE

This publication is a final report by PwC EU Services of the *Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118* as part of the implementing framework contract MOVE/ENER/SRD/2020/OP/0008 Lot 6. The document has been elaborated by PwC EU Services in close collaboration with industry experts identified in this publication, and it reflects the results obtained during the elaboration of the study. 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 978-92-68-08397-0	doi: 10.2832/803672	Catalogue number: MI-02-23-118-EN-N

The European Commission is not liable for any consequence stemming from the reuse of this publication.

Luxembourg: Publications Office of the European Union, 2023

EUROPEAN COMMISSION

Directorate-General for Mobility & Transport (DG MOVE)

Directorate B — Investment, Innovative and Sustainable Transport

Unit B4 — Sustainable & Intelligent Transport

Contact: Dr. Saki GERASSIS DAVITE

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

European Commission
B-1049 Brussels

How to cite: European Commission, Directorate-General for Mobility and Transport, *Support Study on the development of a governance framework for the Public Key Infrastructure (PKI) based on the standard ISO 15118*, PwC EU Services, Publications Office, 2023, https://data.europa.eu/doi/10.2832/803672

TABLE OF CONTENTS

Executive summary

The Support Study aims at providing assistance with the planning and **preparation of secondary legislation** (i.e., delegated/implementing act) under the new **Alternative Fuels Infrastructure Regulation** (AFIR)[1]. It describes the **preferred governance and architecture framework for a EU Public Key Infrastructure** (PKI) based on the standard ISO 15118 for the communication between the EV and the recharging infrastructure, including the identification of the policy, governance and technical elements to support it.

To achieve this, PwC carried out the study in **two-phases (Phase 1 & 2)**. In Phase 1, PwC consulted the PKI project developers and service providers involved in the Sustainable Transport Forum (STF) Sub-group on Governance and Standards to help outline and reach an **agreement on the high-level characteristics** of the preferred PKI governance and architecture in the EU. The characteristics are as follow:

- EU-regulated approach (common definitions and minimum market requirements)
- Multi Root-CAs architecture model;
- Interoperability through a Certificate Trust List (CTL) system;
- Mixed approach to governance (i.e., public and private entities involved).

Building on the foundations set in Phase 1, the **Phase 2 of the Support Study, with the support of a dedicated working group of experts constituted in the remit of the STF Sub-group on G&S completed five deliverables** required to set up and operate the EU PKI ecosystem for e-mobility, considering the characteristics summarised above.

The deliverables of this final report are:

- **Deliverable 1** - **Architecture, governance, and operating model** for a EU PKI ecosystem based on ISO 15118 (considering both -2 and -20);
- **Deliverable 2** - **Relevant standards and technical aspects** of the PKI to allow interoperability across multi V2G Root CAs;
- **Deliverable 3** - **Market rules** for the EU PKI ecosystem for e-mobility;
- **Deliverable 4** - **Mutually recognised set of criteria** for Root CAs, subscribers and the CTL of the EU PKI ecosystem for e-mobility;
- **Deliverable 5** - **Implementation plan** for the preferred governance and architecture model;

In terms of main achievements of the study, the most relevant are as follows:

- The **generation of consensus** in a wide and diverse group of stakeholders starting from diverging views on the PKI governance and architecture for the EU, including the concrete use case of Plug & Charge;
- **Definition of the main features of a future EU PKI ecosystem for e-mobility** in relation to ISO 15118;
- Development of an agreed upon **set of definitions for the EU PKI ecosystem for e-mobility;**

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1804&qid=1695369930667

- **Definition of a proposed governance and architecture** framework for the potential future EU PKI ecosystem for e-mobility;
- Definition of a **clear way forward to fill the standardization gaps of an interoperable architecture based on the CTL**, including:
    - New **European Commission standardisation request** to ETSI to cover the EU PKI CTL requirements;
    - **Agreement to work with EU industry through the OPNC taskforce** within CharIN to address other relevant standardisation aspects;
    - **Upcoming coordination with STF Sub-group on Governance & Standards for further endorsement and submission of OPNC** to international standardization organization (IEC or ISO).
- **Draft of a new full set of market rules for the EU PKI ecosystem**, its participants (PKI Systems, PKI operators, Root CAs, OEMs, CPOs, EMSPs, Certificate Pools and Services), and the EU Governance components (ePEGMB, CTL, TLM, ePOC, EPEOB), considering input by relevant stakeholders;
- **Definition of the structure of the delegated/implementing act** under AFIR for the establishment and operation of the EU PKI ecosystem for e-mobility and the draft contents of the related annexes.

The Support Study aims to represent the overall development of an innovative work, based on an open public and private dialogue and cooperation, that could serve also as a **reference for other regions** for the creation of **open and freely competing e-mobility markets** based on common rules and definitions. In order to bring forward the progress achieved during this Support Study we have identified a series of steps, listed below, that will be necessary in order to s**et-up the EU PKI for e-mobility** and **ensure its full implementation**:

- **Fine-tuning and conclusion with industry experts on** a number of outstanding technical aspects that are in advanced state of development after the Support Study **(i.e., security policy, certificate policy and onboarding guidelines);**
- Adoption by the EC of the **relevant delegated and implementing acts** in support of the EU PKI ecosystem for e-mobility;
- Set-up of **an expert group for the future e-mobility PKI governance and management body;**
- Development by European/International Standardisation Organisations and market actors of the **CTL technical specifications** and **relevant protocols** for the functioning of the EU PKI ecosystem;
- Start of the **technical work on the EU PKI CTL interoperability by EC (or delegate such as JRC).**

Abbreviation List

AFIR – Alternative Fuel Infrastructure Regulation
AFIREV – Association Française pour l'Itinérance de la Recharge Électrique des Véhicules
API – Application Programming Interface
C-ITS – Cooperative Intelligent Transport System
CA – Certification Authority
CC – Cross-Certification
CEF – Connecting Facility Europe
CP – Certificate Policy
CPO – Charge Point Operator
CPS – Certificate Practice Statement
CR – Cross-Recognition
CRL – Certificate Revocation List
CS – Charging Station
CTL – Certificate Trust List
C-ITS – Cooperative Intelligent Transport System
DSO – Distribution System Operator
EMSP – e-mobility Service Provider
EC – European Commission
ePEGMB – European PKI Ecosystem Governance and Management Body
ePEOB – European PKI Ecosystem Operating Body
EPOC – e-mobility Point of Contact
ETSI – European Telecommunications Standards Institute
EV – Electric Vehicle
EV-OEM – Electric Vehicle Original Equipment Manufacturer
EVSE OEM – Electric Vehicle Service Equipment Original Equipment Manufacturer
EVSE – Electric Vehicle Supply Equipment
IEC - International Electrotechnical Commission
ISO – International Organization for Standardization
JRC – Joint Research Centre
MSP – Mobility Service Provider
OCSP – Online Certificate Status Protocol
OEM – Original Equipment Manufacturer
PnC – Plug&Charge
PKI – Public Key Infrastructure
RA – Registration Authority
R&D – Research and Development
SECC – Security Evaluation & Certification Consortium
SP – Security Policy
STF – Sustainable Transport Forum
STF Sub-group on G&S - Sustainable Transport Forum Sub-group on Governance and Standards
TBC – To be confirmed
TBD – To be determined
TLM – Trust List Manager
TLS – Transport Layer Security
ToR – Terms of Reference
V2G – Vehicle-to-Grid
WG – Working group

1 Introduction

This document is the Draft Final report for the **Support Study on the development of a governance framework for the Public Key Infrastructure (PKI) based on the standard ISO 15118**. The study is aimed at supporting the **planning and preparation of secondary legislation under the Alternative Fuels Infrastructure Regulation (AFIR)**, describing the preferred governance and architecture option for the establishment and operation of the EU PKI ecosystem for e-mobility as well as identify the policy, governance and technical elements to support it.

The Support Study, being carried out hand-in-hand with the **Sustainable Transport Forum of the European Commission - DG MOVE**, has been structured in two phases, with different methodologies and outputs as briefly described in the table below.

Table 1: The Support Study's phases

Study phase	Aim	Timeframe	Methodology	Output
Phase 1	Definition of high-level requirements of the EU PKI ecosystem for e-mobility in relation to ISO 15118	Sept. '22 – Jan '23	Interviews with PKI project developers and service providers of the STF Sub-group on G&S[2] and checkpoints with the STF Sub-group on G&S	4 recommendations on the high-level specifications on the EU PKI ecosystem for e-mobility
Phase 2	Development of detailed set of deliverables to support the EC in the development of secondary legislation under AFIR, including the set-up of a future interoperable architecture	Jan. '23 – Jun '23	Working group of experts[3] meeting once per week to elaborate and review a set of detailed deliverables	6 deliverables on policy, governance and technical elements to support the PKI ecosystem for e-mobility

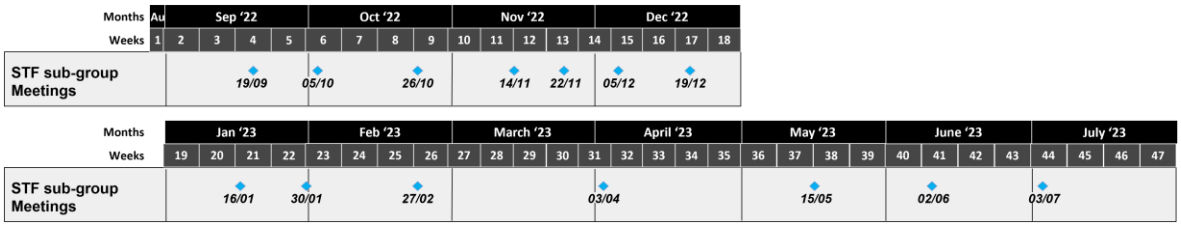
This report describes the **detailed methodology adopted in the two phases of the Support Study, highlights the main findings based on the recommendations of Activity 2 - Block 2 'Development of a governance and architecture framework** for the implementation and operation of a **PKI ecosystem for e-mobility in the European Union'[4],** and introduces the **deliverables produced** based on the aforementioned recommendations to support the **preparation of the secondary legislation under AFIR and the expected technical set-up of a EU PKI ecosystem for e-mobility**, announced by the European Commission during the STF

[2] Namely: CharIN, Gireve, Hubject, Vedecom, and SAE.
[3] PKI project developers and service providers, CPOs, OEMs, PKI service providers, energy generation companies, etc.
[4] Document drafted by the STF aiming at reaching a consensus between the members of the sub-group on the choice of a governance framework and PKI architecture for vehicle-to-grid communication, defining its ownership model as well as the roles and responsibilities of every type of market player: https://op.europa.eu/en/publication-detail/-/publication/b7910659-276c-11ee-839d-01aa75ed71a1/language-en

Plenary on 2 June 2023, to be carried out as of January 2025 by the European Commission's Joint Research Centre (JRC).

The Gantt chart, including the meetings with the STF Sub-group on G&S, can be found below:

Figure 1: Gantt of the appointments with the STF Sub-group on G&S



It is important to mention that the document includes a detailed description of **the process** that the Support Study and the European Commission followed to **achieve consensus among stakeholders** for the establishment of the EU PKI Ecosystem for e-mobility and the **deliverables required for its set-up and operation**. That successful approach could also be used by **other markets to replicate this process** looking to set-up a PKI ecosystem for e-mobility that could be interoperable at global scale.

2 Phase 1 – Definition of high-level specifications

The first phase of the Support Study, covering the period from September 2022 to January 2023, was aimed at **mapping the views and position of the PKI project developers and service providers present in the STF Sub-group** on **Governance and Standards** – namely CharIN, Gireve, Hubject, Vedecom, and SAE[5] – on **fundamental topics** the industry has been discussing for long (see table below).

Table 2: Aspects covered in Phase 1

#	Title	Description
1	**PKI interoperability**	Facilitating, securing and optimising certificates and data exchanges between charging infrastructure operators and mobility operators
2	**Governance & architecture**	Definition of a PKI architecture and a governance model
3	**Ownership model**	Definition of roles and responsibilities for the actors included in the architecture of the PKI ecosystem
4	**Implementation scheme**	Identification of a plan to implement the governance and architecture of choice

[5] Observer to the sub-group and invited by the European Commission

Phase 1 has been carried out hand-in-hand with the **Sustainable Transport Forum** (STF) Sub-group on Governance and Standards, building on the recommendations of said group and complementing them with an **additional set of recommendations**, which then acted as a guideline to define all technical aspects in later stages of the assignment. Specifically, in Phase 1 PwC, in collaboration with the interviewed stakeholders, built the base upon which the Support Study has been developed during Phase 2 (exact details on Phase 2 are given in Chapter 3).

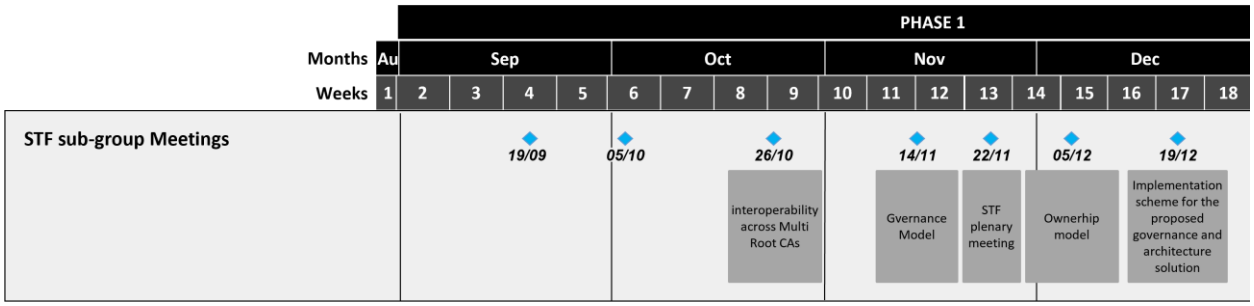
The splitting of the Support Study in two phases, which was procedurally agreed together with the European Commission, was due to a perceived need to **concretise the positioning of PKI project developers and service providers to create areas of consensus regarding the key topics** mentioned above. This was considered fundamental, before moving into the discussion and development of detailed technical aspects of the governance and architecture, as done in Phase 2.

2.1 Methodology for Phase 1 of the Support Study

The methodological process applied during the first phase has been named '**consultation sprints':** hence, a series of regular interviews, based on a structured and agreed questionnaire with the European Commission, were carried out between the recurring STF Sub-group meetings to collect the relevant contents on each topic. Starting from the STF sub-group meeting on October 5th, 2022, PwC started to engage with relevant stakeholders so as to **report the results achieved through these consultations in the STF meetings taking place from October to December 2022**. These consultations, served to collect high-level perspectives from stakeholders, and allowed PwC and the European Commission to move the discussion forward with industry stakeholders on the key topics under discussion, triggering a common positioning and joint preference by player in the EU PKI ecosystem.

The first part of the assignment followed the timeline outlined by the Gantt chart below.

Figure 2: Gantt Chart – Phase 1



Stakeholder mapping

In accordance with the European Commission the main stakeholders engaged have been the **PKI project developers and service providers of the STF sub-group,** namely: **CharIN**, **Hubject**, **Gireve, SAE and Vedecom.** However**,** in the execution of the assignment, to offer a **comprehensive and broad perspective**, PwC engaged also with a number of additional stakeholders, to gather further information on the main topic addressed in phase 1 of the study (see paragraph 2.3), as well as **to bring in the STF sub-group discussion examples of best practices** in the PKI sphere.

Description of the current EU PKI ecosystem

The PKI project developers and service providers represented the **primary stakeholders engaged in phase 1** of the Support Study, in line with the requests of the European Commission. The following table provides a company description of the PKI project operators consulted during phase 1.

Table 3: PKI project developers and service providers of the STF Sub-group on G&S

Logo	PKI Partner Description
CHARIN	CharIN is an **industry organisation** than incudes several PKI operators, OEMs, CPOs as well as other players form the PKI ecosystem. Most notably within CharIN there are two communities dealing with PKI/PnC topics: **Task Force PKI** and **PnC Project Europe**. The former is a workgroup focussed around technical discussions and **definitions on security topics and interoperability of a PKI** (i.e., Certificate Policy Guideline, identification and description of use cases within the PnC Ecosystem which are not yet clarified by existing standards and related documents). The PnC Project Europe stive for the **setup of a PKI to enable secure authentication and authorization via Plug & Charge in accordance with ISO 15118**, with CharIN covering the role of the proposed operator and provider of required services.
Gireve	Gireve is a **service provider operating in the PnC ecosystem and in relation to ISO 15118** since 2018. The service offered are **certificate issuing**, **certificate-authority** roles, and **pool management**. Gireve is part of the **Mobena project**, which aims at **fostering the deployment of ISO 15118 and PnC**, as well as contributing to several standardisation bodies and specification working groups to promote and advance standardisation.
HUBJECT	Hubject GmbH is a **joint venture** formed by the BMW Group, Bosch, Daimler, EnBW, RWE and Siemens, which operates a PKI in the e-mobility sector since 2018, with the purpose of enabling the worldwide use of PnC by implementing the ISO 15118-2 standard. Its **eRoaming platform** enables Charging Point Operators (CPOs) and e-mobility Service Providers (EMSPs) to access the charging infrastructure regardless of any network.
SAE INTERNATIONAL	SAE is a global association connecting and educating mobility professionals to enable safe, clean, and accessible mobility solutions. SAE EV Charging PKI project aims at **design and test a worldwide EV charging industry PKI platform**. To pursue that objective the project operates an **industry-led, pre-competitive research** to strengthen electric vehicle charging system security.
INSTITUT VEDECOM	Vedecom's initiative **Mobena project gathers 20 partners** including 19 industrials representing the mobility sectors. In the context of the Mobena project the following action are pursued in a **collaborative framework** within working group and will be published at the achievement of the projects' milestones: • **Definition of a transition roadmap towards new generation charging solutions** and use cases, including Plug and Charge 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

As aforementioned, in addition to the organisation above, PwC engaged with a selection of additional stakeholders, as described below.

Table 4: Additional stakeholders

Name	Description
European Commission	
Joint Research Centre	Under suggestion of the European Commission, the JRC was consulted on several occasions to tap into its expertise gained through the **Cooperative Intelligent Transport System (C-ITS)** initiative. The C-ITS allows cooperation between two or more ITS sub-systems (personal, vehicle, roadside and central) to offer **enhanced communication between vehicles**, transport infrastructure and people to **provide information, warning, and assistance services**.
Other industry stakeholders	
STF Sub-group on G&S - Block 3 participants	PwC in multiple instances had joint and individual conversation with Block 3's STF sub-group members (i.e., ChargePoint, CharIN, EnBW, Hubject, Shell, Tesla). The Block 3 is dedicated working group within STF SG1 focusing on **regulatory needs and other open issues** within the e-mobility ecosystem. The issues it covered were mostly triggered by Activity 1 of STF SG1. The purpose was to **create synergies** among the Support Study and the activities falling under the scope of Block 3. Additionally, Block 3 members were important contributors to the progress of the study by **providing feedback on PwC's presentations** on the findings of the consultations.
Visa	Visa reached out to PwC in order to take part in the consultation. PwC involved Visa in the consultations when collecting information on best practices in other sections, more specifically to gather insight on the **VISA's PKI used to authenticate payments across their network**.
DigiCert	DigiCert was involved in the consultation process due to its connection to one of the main stakeholders, SAE. From the interaction with DigiCert, PwC gathered significant **technical insights regarding the operation of PKIs** as well as some **best practices** coming from different sectors (i.e., Matter, NG911).

Topics addressed during consultations

In the period between October and December 2022, PwC carried out **four rounds of consultations**. Each round covered one specific recommendation of the STF sub-group's document Activity 2 Block 2, in particular recommendations 3 to 6. Recommendations 1 and 2 had already been tackled and agreed upon by the European Commission with industry stakeholders prior to the beginning of the Support Study.

The entire **list of recommendations covered in Activity 2 - Block 2** is reported in the table below.

Table 5: List of recommendations covered in Activity 2 – Block 2

Recommendation	Recommendation
1	A regulated vs. non-regulated governance and architecture
2	Single vs. Multi-Root CA model
3	Interoperability across Multi Root CAs
4	Governance and architecture
5	Ownership model
6	Implementation scheme for the proposed governance and architecture solution.

**In black the recommendations concluded in in the STF before the PwC Support Study started.*

Chapter 2.2 contains an in-depth **breakdown of the findings** of the consultation process for each recommendation. Overall, the contents of the six recommendations covers the **main topic to address in setting up a functioning and interoperable PKI**.

Consultation tools of Phase 1

Table 6:Consultation tools of Phase 1

Tool	Description	Targets	Timing	Output
Interviews	Collect the positions of PKI project developers and service providers on fundamental topics of the PKI and collect relevant insights on the PKI from other stakeholders	PKI project developers and service providers, Activity 2 - Block 3[6] coordinators[7] and a selection of external stakeholders[8].	October '22 – December '22	• Insight collection • Preferences mapping
STF sub-group meetings on Governance and Standards	Validate the contents gathered during the interviews	STF sub-group G&S	October '22 – December '22	• Feedback and insight collection • Validation of the information

For the execution of the first portion of the assignment (i.e. Phase 1), in accordance with the European Commission, the interviews were deemed the most suitable consultation method. Further details of this approach are provided below.

Interviews

Each round of consultations focused on one of the specific recommendations (specifically from 3 to 6) described above. On the basis of an ad-hoc questionnaire developed for each recommendation, PwC guided the interaction with the interviewee and encouraged responses that would favour **comparisons and additional analysis. The data collection process with interviewees mainly occurred through virtual meeting, however,** stakeholders were requested to provide **written answers to the questionnaire** for the sake of achieving a complete and comprehensive picture whenever they were not available.

STF Sub-group meetings on Governance and Standards

After each round of interviews**, PwC processed the answers** and, whenever possible, **different stakeholders' views where aggregated to obtain a common one**. The content gathered through the interviews was then reflected into a deck of slides which was subsequently presented to the **recurring STF sub-group workshops to validate it through the members**, **stimulate discussions in the meetings** to gather additional inputs, as well as to **collect their feedback** on the topics and the conclusions reached.

---

[6] With Activity 2 Block 3 the STF aims at addressing several follow-up topics within the discussion concerning standards and protocols for communication exchange in the electromobility ecosystem emerged from Activity 1.
[7] ChargePoint, CharIN, EnBW, Hubject, Shell, Tesla.
[8] JRC, DigiCert, Visa.

In the table below, we provide an overview of the timeline of consultation methods carried out in this phase, hence the interviews and the recurring sub-group workshops.

Table 7: Timeline of recurring STF sub-group workshops

Consultation sprint	Topic	Consultation Tool	Start date	End date
Sprint 1	**Recommendation 3 - interoperability across Multi Root CAs**	Interviews	06/10/2022	25/10/2022
		Recurring STF sub-group workshop	26/10/2022	n.a.
Sprint 2	**Recommendation 4 - Governance model**	Interviews	27/10/2022	13/10/2022
		Recurring STF sub-group workshop	14/11/2022	n.a.
Sprint 3	**Recommendation 5 – Ownership model**	Interviews	15/11/2022	04/12/2022
		Recurring STF sub-group workshop	05/12/2022	n.a.
Sprint 4	**Recommendation 6 – Implementation scheme**	Interviews	06/12/2022	18/12/2022
		Recurring STF sub-group workshop	19/12/2022	n.a.

2.2 Results achieved in Phase 1

The focus of the first portion of the Support Study was centred around assisting the European Commission in **capturing and consolidating the content** for the completion of the STF G&S's deliverable under **Activity 2 Block 2**. The deliverable is structured in **six recommendations** regarding the **main aspects required to set up a PKI architecture**. **The first two recommendations were developed jointly by the European Commission and the STF sub-group members**, before the beginning of the Support Study. PwC instead**, through the stakeholder consultation process, contributed to the finalisation of recommendations 3 to 6**.

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

Analysis by the STF Sub-group on G&S

The first recommendation of Activity 2 Block 2, developed by the STF sub-group members **prior the initiation of the Support Study,** regarded recommending **whether the governance and architecture of the e-mobility PKI should be regulated or not**. In the case of the **regulated approach,** the implementation and development of **common requirements for the operation and development of the e-mobility PKI** on important aspects such as interoperability as well as governance and architecture would be required; on the other hand, the **non-regulated approach leaves the market independently in charge of the formation and development of the e-mobility PKI**.

Conclusions on the regulated vs. non-regulated governance and architecture

The preference of the members of the STF sub-group resulted being the **regulated approach** to the governance and architecture in Europe due to the advantage of providing a clear legal basis covering key elements of the PKI. The secondary legislation under AFIR therefore, should include a series of **minimum policy, technical and operational requirements** with the purpose of ensuring **an open, interoperable, and competitive PKI ecosystem in the EU**.

Lastly, it is important to note that **some of the more operational aspects of operating a PKI (i.e., PKI systems and associated services) can be better addressed directly by the industry**. In fact, the preference of STF sub-group members of governance and standard is for the regulation to establish the minimum requirements and **let the industry-led innovation to bring services forward to the market.**

Recommendation 2: Single or Multi Root CA model

Analysis by the STF Sub-group on G&S

The second recommendation, also developed by the STF sub-group members **before PwC's involvement,** addressed the set-up of a **single vs. multi-Root CA model**, with the aim of achieving an open and interoperable PKI for e-mobility.

The **Single-Root CA model** would consist of a European PKI characterised by the presence of **only one V2G Root CA**. This solution would not match the real market scenario where several market actors have the intention to develop their V2G Root CA, thus, having a single V2G Root CA would imply significant limitations. As a result of that, it arises the need of **achieving interoperability** across Multi-Root CAs, while reducing the complexity and costs of the PKI, but allowing multiple market actors to interact and offer their services.

In addition, a Single-Root CA model may also lead to the following specific **issues:**

- the risk of **abuse of dominant position** in the market by the single entity operating such an important role in the PKI system as the Root CA. Competition may benefit the whole market by means of increased quality, consumer freedom of choice and decreased prices;
- **Single point of failure**, when if the single Root CA goes down (i.e., technical issues, cyber threats, etc.) the whole PKI system would come to a halt.

The **Multi Root CA model** significantly **reduces the risk** linked to the single point of failure by introducing **redundancy-related resilience** in the system. In this case in fact, in the event of technical issues with one Root CA, other Root CAs could continue to handle the operations with minimal disruptions. Also, the risk of abuse of dominant position would be drastically reduced and **competition among businesses** is expected to also **drive up the service quality while promoting affordable prices**. These advantages, however, would be counterbalanced by **an increase in complexity and costs** at the ecosystem level due to the necessity of ensuring interoperability across the different trusted Root CAs.

Conclusions on the single / multi root CA model

The STF sub-group members advocate for a multi-Root CA model due to the **benefits of having competition in the market** among several V2G Root CAs – **increased variety and quality of service, reduced prices** - as well as the **increased operational resilience of the**

PKI ecosystem. The recommendation is also in line with the **commitment of multiple players in the European market to offer V2G Root CA** services (e.g., CharIN, Hubject, Gireve). However, **interoperability** between these multiple V2G Root CAs must be ensured. Consequently, secondary legislation under AFIR should include **interoperability requirements to ensure functionality and security of the PKI ecosystem** for e-mobility so that the potential PKI systems (and relevant V2G Root CAs) can function in any vehicle and recharging station.

To foster interoperability, regardless of the chosen interoperability solution, encouraging a comparable level of security among CAs is an important aspect. The regulation, for instance, could promote this through the **development of a common set of criteria that each** PKI system should follow.

Recommendation 3: Architecture model to ensure interoperability across Multi Root CAs

This recommendation is a direct consequence of Recommendation 2 as it regards **interoperability across Multi Root CAs**, defined as a **facilitating, securing and optimising certificates and data exchanges between charging infrastructure operators and mobility operators**[9]. This is a key feature to ensure that the relying party of a transaction or message can evaluate whether to accept or reject that transaction[10].

Thus, to achieve PKI interoperability, two processes are needed:

- A **contractual process** to establish that a given PKI system (V2G Root CA) meets certain technical and management interoperability requirements;
- A **technical mechanism** to convey sufficient information about the standing of a given PKI system, as established by the first process, in a machine-readable form, so that receivers of digital certificates can automatically decide whether or not to accept them.

No PKI project developer and service provider at the time of the interviews had an interoperability solution available for the market, and its potential scale-up. Most of them were in the stage of **testing solutions** in order to be **ready to implement them with increasing demand in the market**. In addition to this, the industry faces the challenge of agreeing on a common interoperability solution, with actors initially supporting different interoperability options. At the moment of initiating this Support Study and discussions in the STF Sub-group on Governance & Standards there was not market consensus.

Analysis of the interoperability options

Through a combination of consultations and desk research, the following possible solutions which could allow interoperability among e-mobility PKIs were identified:

- **Cross-certification (CC);**
- **Cross-recognition (CR);**
- **Certificate Trust List (CTL).**

Each option is described in detail in the following sections.

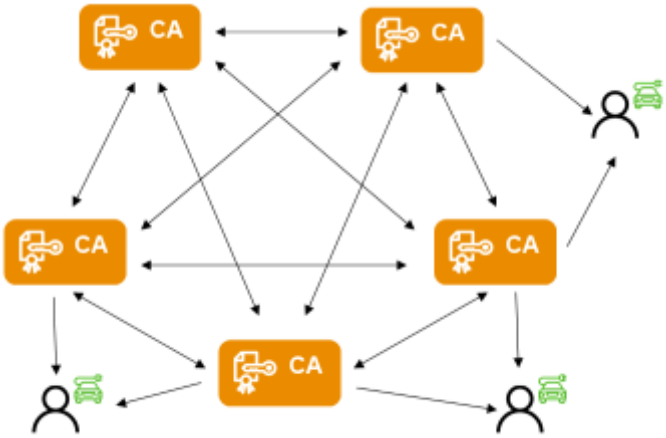
---

[9] Ibidem.
[10] Connolly, C., van Dijk, P., Vierboom, F., Wilon, S. (2005). PKI Interoperability Models. Accessed on December 22nd, 2022 from: https://www.galexia.com/public/research/assets/pki_interoperability_models_2005/pki_interoperability_models_2005.pdf

Cross-certification (CC)

As illustrated in the picture below, Cross-certification represents a **peer-to-peer approach to interoperability**, meaning that **CAs in the ecosystem bi-laterally choose whether or not to trust each other**. Consequently, interoperability is **handled by PKI operators**. If the link of trust is established among CAs, they issue cross-certificates to one another. This mechanism allows users to trust unknown CAs by **tracing the certificate issued by them back to a trusted CA**. This can be done by enabling users to access their trusted CA's certificate repository or 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[11].

Figure 3: Cross-certification (CC)



Cross-certification has been the subject of several testing events among several PKI operators in Europe. The solution is **technically simple to set-up** as there is already technical know-how in the industry. Moreover, **the time needed to set it up is relatively fast as it is dependent on bilateral agreements among the market players**. In respect of ISO 15118, Cross-certification is compatible with both ISO 15118-2 and ISO 15118-20. The main issue that emerged for this option is related to the **scale up process**. More specifically, **as the number of Root CAs grows, the number of cross-certificates also grows:** in fact, upon entrance of a new V2G Root CA, two additional cross-certificates are required for any incumbent Root CA[12].

This renders a PKI, based on Cross-certification, **difficult to operate when the number of V2G Root CAs goes beyond a certain limit**. Furthermore, **as the adoption of the Cross-certification would require changes to the software of EVs and CSs**, the need for maintenance would increase, especially for handling cross-certificates in the system. For a secure interaction among EVSE and vehicle, the EVSE must have in storage the n*(n-1)/2 cross-certificates while the EV only need to store one. This will also imply that the onboarding of

[11] Elaad. (2022) Public Key Infrastructure for ISO 15118 Freedom of Choice for Consumers & an Open Access Market. Accessed on December 22nd, 2022, from: https://elaad.nl/en/new-pki-publication-freedom-to-join-the-charging-infrastructure-of-the-future/

[12] Ibidem.

a new Root CA would result in additional effort being imposed once per Cross-certification relation.

Another issue that might emerge with this interoperability option is known as the "**partial mesh"**: this arises when **some of the Root CAs in the network do not directly cross-certificate with one another**. In this case **the trust of the whole system is compromised** due to the extension of the trust boundaries and an overall increase in risk. The problem is linked to the fact that for each certificate verification the entire chain of CAs must be trusted, which can make it become excessively long. In this 'partial mesh' it may become necessary for users to have a way of limiting the chain of certificates that can be used to verify a signature. Due to these relevant issues, the Cross-certification might not be the optimal approach to establish a wide-spread European (or global) PKI. Instead, Cross-certification is most suited where two or three related CAs are required to interoperate with each other.

Cross-recognition (CR)

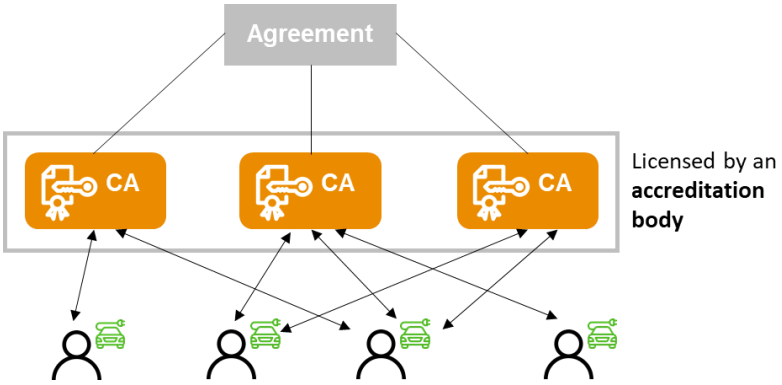
Cross-recognition occurs when **an individual CA or an entire PKI domain recognises another CA or PKI domain**[13]. Therefore, to achieve interoperability based on Cross-recognition a **strong cooperation among several actors** is necessary as it is handled by PKI operators. The solution **allows final users to rely upon certificates issued by the recognised CAs**. This is achieved thanks to PKI authorities of different domains acting as **trust points**, formally and reciprocally recognising each other's capacity to manage and enforce PKI standards as well as trust processes to accept certificates.

Cross-recognition requires a **strong collaboration among the various actors in the market** in order to achieve the required level of trust which ultimately allows them to recognise one another. To this purpose, the presence of a neutral and accepted coordinated authority could help reaching an agreement on the common set of criteria that CAs have to comply to in order to be recognised as trustworthy.

Due to its nature, it **could be set up relatively in a short period of time when the number of players in the PKI domain is contained** but the large need for cooperation might result in **issues related to the scalability** of the solution as the number of players rises. This can be addressed by establishing an **accreditation authority** licensing the independent CAs on the basis of a set of mutually recognised criteria. Consequently**, the users' trust in the accreditation authority would be reflected upon the certificates emitted by the recognised CAs**.

[13] Connolly, C., van Dijk, P., Vierboom, F., Wilon, S. (2005). PKI Interoperability Models. Accessed on December 22nd, 2022 from: https://www.galexia.com/public/research/assets/pki_interoperability_models_2005/pki_interoperability_models_2005.pdf

Figure 4: Cross-recognition (CR)



Compared to Cross-certification, Cross-recognition's main distinction lies in the **nature of the relationship among CAs**: the Cross-recognition is not based on a set of bilateral (or even unilateral) agreements between CAs. In this instance, the **trust in foreign CAs is ensured by being licensed by the accreditation body**. Alternatively or complementarily, being **audited by a trusted independent party** might be sufficient.

When it comes to scalability, Cross-recognition and Cross-certification share the same issue. In this case however, the issue lies where the interoperability is handled. For Cross-recognition, the interoperability occurs at EV level (for Cross-certification it is handled outside the EV, at CSs level). As a consequence the devices - EVs and CSs - must install and periodically update the set of recognised V2G Root CAs. This process, particularly from the EV's perspective, can be particularly challenging, as currently the only solution is for OEMs to physically recall vehicles to proceed with this update. In addition, when a new V2G Root CA enters in the market, all existing devices must be updated. However, the onboarding of a new Root CA requires a **one off-effort**. In fact, even though it is a time-consuming process, the addition of a new CA must only be done once as the certificate signed by the new CA will be trusted as long as it validly licensed by the accreditation body.

Although Cross-recognition does not experience some of the technical interoperability issues of Cross-certification and is suitable for both ISO 15118 version (i.e. -2 and -20), nevertheless it still experiences the same **administrative and management issues of establishing and maintaining trust in the whole network when this increases over time** (i.e., ensuring that all CAs recognised by the others, ensure that the interoperability pertains with an increased number of CAs, etc.).

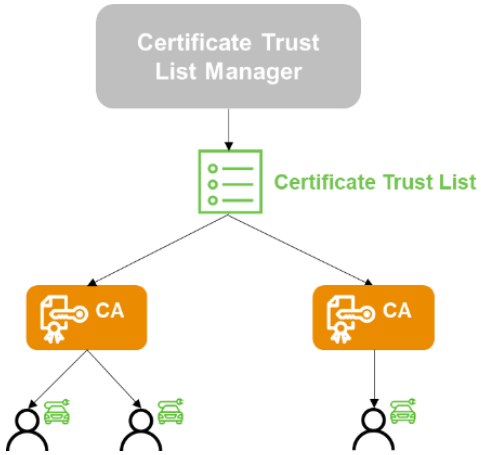
Certificate Trust List (CTL)

As illustrated in the picture below, the Certificate Trust List (CTL) consists in a **predefined list of items that has been signed by a trusted entity**. This type of interoperability solution gave rise to the "Browser model", or in other words, the most diffused interoperable PKI in a plethora of browser applications (i.e., Chrome, Firefox, etc.). The CTL in fact, is a straightforward method that generates trust in the PKI domain as the **relying parties and the CAs need only to trust the issuer of the CTL** which consequently allows the CAs included in the list to be trusted by all actors. Said issuer is called **Trust List Manager** (TLM) and it is responsible for **publishing and maintaining** the list of certificates (progressively updating it including certificated form new CAs and removing the revoked certificates). The TLM has a central role that must be trusted by all

companies and systems in the market that are using the CTL. The TLM has strictly a governance role and does not have a business involvement in the PnC market[14].

The CTL, unlike Cross-certification and Cross Recognition, it adopts a centralised approach. Thus, the CTL works by maintaining and distributing a list of V2G Root CA certificates that are trusted in the market to EVs and charging stations.

Figure 5: Certificate Trust List (CTL)



The CTL **could be implemented with ease with existing protocols,** as it was **tested in demos and testing events**. When compared with other options in fact, the CTL implies a **reduced operational complexity** as it does not have major impacts to software of EVs and CSs. Specifically, the CTL fits within current logic of the certificate verification (algorithms, software, etc.) although on the other hand it requires a **demanding set up**. In this regard, before tackling the actual technical solution, two important aspects would need to be clarified:

- the **entity responsible for the management of the CTL** would need to be identified;
- the **set of mutually recognised criteria to include** (and exclude) **V2G Root CAs in the list** would need to be determined.

Furthermore, **the CTL would need to be embedded in every device of the ecosystem** and will require **periodical updates** in order to be secured and trusted. The update process would be centralised mainly on the TLM, and it consists in removing from the CTL the revoked certificates as well as including the certificates of new trusted CAs. In exchange for the implementation complexity, the **CTL would be able to scale up without resulting in particular technical issues**, unlike the other interoperability options. Lastly, the CTL is a feasible option within the context of ISO 15118 (possibility also of coexistence, if needed, of V2G Root CAs based both on ISO 15118-2 and -20). One notable implication of achieving interoperability through the CTL is the need for an initial economical investment in order to be set up.

[14] Elaad. (2022) Public Key Infrastructure for ISO 15118 Freedom of Choice for Consumers & an Open Access Market. Accessed on December 22nd, 2022, from: https://elaad.nl/en/new-pki-publication-freedom-to-join-the-charging-infrastructure-of-the-future/

Conclusions on interoperability

Interoperability it is not a purely technical problem. Alongside the choice on the most suitable technical solution, there is the need for business agreements among the market actors. Both considerations should be taken into account when deciding which interoperability solution to adopt. In this respect, a CTL approach is the preferred solution by PKI operators and service providers of the STF sub-group on G&S.

The root cause of this preference was found in the **scale-up advantage that the CTL carries against the other two interoperability solutions** (Cross-certification and Cross-recognition), particularly in view of the inability either for the market or the regulator to **predict or prescribe a maximum number of V2G Root CAs**. This assumes a particular relevance **considering that all PKI project developers and service providers consulted would favour a single interoperability solution to be uniformly adopted throughout the market**. Having multiple interoperability options co-existing simultaneously, for example CTL and Cross-certification, albeit possible form a technical standpoint, it may lead to the **creation of "islands" of interoperability**.

Moreover, the STF sub-group members oh G&S expressed a general preference for the **CTL** as the interoperability solution across the **Multi-Root CA** model. This results from the **potential for scalability**, centralised maintenance, and fitting logic of certificate verification. Although CharIN is open to the CTL, it suggested Cross-recognition as a potential alternative solution. Importantly, **there is a strong preference for the CTL interoperability option to be compatible and adaptable within the framework of ISO 15118** for either -2 or -20 versions.

Another point of consensus was **striving for a single interoperability solution to pursue from the early stages of market development** by encouraging V2G Root CAs to achieve **comparable level of trust, reliability, and security**. During the consultation in fact, the **secondary legislation under AFIR emerged as a key tool to realise this** by fostering standardisation under the form of a broader adoption of ISO 15118 and the definition of EU legal provisions sustained by market rules and mandated standards and protocols.

To support the CTL, as well as any other interoperability solution, there is the need to ensure via secondary legislation the use of **ISO 15118 as a minimum indispensable technical standard** as it will contribute to **establish a common baseline for all PKI systems within the EU PKI electromobility ecosystem, in particular for the Plug&Charge use cases** . In addition, it emerged that a set of minimum requirements to ensure that V2G Root CAs could be considered trustworthy and an audit procedure to check the compliance to the criteria would be needed to foster interoperability in the market. Lastly, the secondary legislation could be the ground for the identification of **additional standards** and **technical aspects** to ensure interoperability.

Recommendation 4: Governance model

Recommendation 4 consists in analysing the different governance[15] models for the PKI. Two layers within the governance of the PKI have been identified as described in the following table:

Table 8: Layers of the PKI Governance

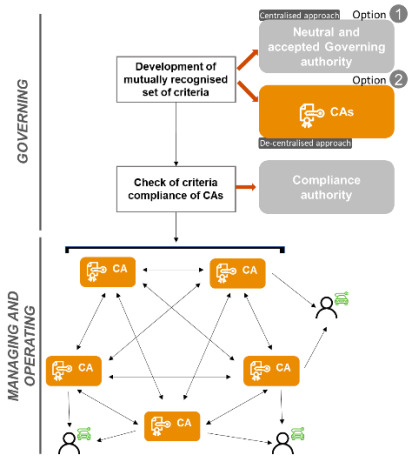
#	Governance layers	Description
1	**Governance layer**	It encompasses the roles required to govern a functioning, fair, open, and non-discriminatory PKI, including: 1. **Criteria definition:** Definition of criteria that V2G Root CAs must conform to be considered trustworthy, including Certificate Policy criteria, technical requirements and legal requirements; 2. **Check of the criteria conformance:** Check the Root CAs conformance to the established criteria to ensure trust in the ecosystem; 3. **Publish the Trust List (only applicable for the CTL):** Publishing and managing the Trust List is the last governance role, albeit it is only applicable if the Certificate Trust List is the chosen interoperability option.
2	**Managing and operating layer**	The managing and operating layer addresses the operations of the PKI, thus the actual provision of the emission of certificates and signing service to ensure interoperability.

Analysis of the PKI governance

Governance models

On the basis of the two governing layers described above, a governance model has been developed for each interoperability solutions explored in Recommendation 3. The table below provides a description of each model.

Governance model for PKI interoperability through Cross-certification (CC)



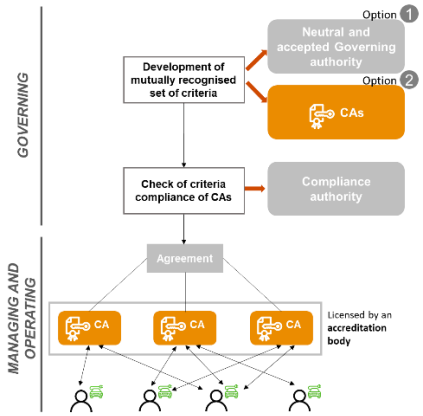
The **governing layer** comprises the first governance block regarding the development of mutually recognised set of criteria for V2G Root CAs to be considered trustworthy. This block could be addressed in two approaches: (1) A **centralised approach** which foresees the definition of criteria by a neutral and accepted governing authority; (2) Or a **decentralised approach** in which the CAs themselves collaboratively define the criteria.

To ensure the V2G Root CAs involved are trustable, the **second governing block envisages a compliance checking authority** to scrutinise the CAs in order to verify their compliance to the mutually recognised set to criteria.

At the **managing and operating level there are bilateral relationships among the V2G Root CAs and their connections with the final users**. Thus, the Cross-certification features a **local governance with a peer-to-peer approach**.

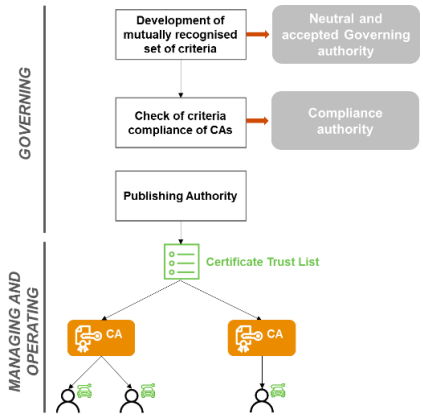
[15] Defined as: the act to process of governing or overseeing the control and direction of something (in this case the PKI).

Governance model for PKI interoperability through Cross-recognition (CR)



The governance model for **Cross-recognition**, at the **governing layers it is structured in the same way as the Cross-certification** and the definition of criteria to determine the trustworthiness of CAs can be addressed with a centralised or decentralised approach. In addition, it foresees the involvement of a compliance authority to perform the second governance block of checking the V2G Root CAs compliance to the criteria. **The main differences occur at the managing and operating level**. Here, two fundamental elements characterise the Cross-recognition: the first is the **definition and adoption of a common agreement among the recognised CAs**. It includes the mutually recognised set of criteria and additional technical and security specifications that the CAs commit to comply to. The second element is the presence of a **licensing/accreditation authority** that harnesses the trust of all market actors, emitting licenses/accrediting the CAs respecting the defined set of trustworthiness criteria.

Governance model for PKI interoperability through Certificate Trust List (CTL)

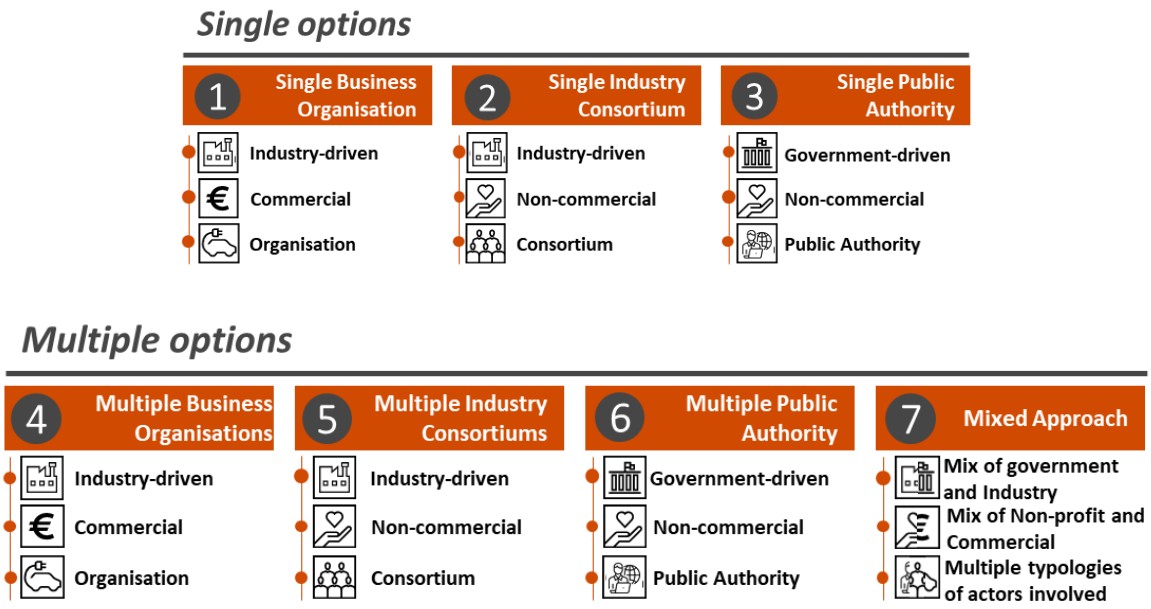


The last governance model addresses the preferred interoperability option among the PKI project developers and service providers, the **Certificate Trust List**. At **managing and operating level**, the underlying mechanism is rather simple as **the V2G Root CAs' certificates included in the Trust List are trusted by all players in the market**. The main difference with the other interoperability solution occurs at the **governing level**. The **first governance block**, namely the definition of criteria, can only be **performed with the centralised approach**, thus by a neutral and accepted governing authority. The model also foresees the involvement of a **compliance checking authority** addressing the second governance block as for the previous options. The CTL however includes a third block, which concerns the **publishing and managing of the list of trusted CAs**. This function is performed by an entity called **Trust List Manager** (TLM). It generally appointed by the same neutral and accepted governing authority responsible for the definition of criteria. In this case this authority is also in charge of the definition of rules and responsibilities regulating the operations of the TLM.

Governance options

The purpose of the consultation for recommendation 4 was to address the different **governance options**, hence, **which kind of organisations** – private companies, industry consortia, and public authorities – should be **involved in the governance of the PKI**. To perform this analysis PwC identified firstly a **number of governance options**, described in the following figure.

Figure 6: Governance options (Single & Multiple)



Single options

The single governance options prescribe a **single entity governing and operating the PKI**. Said entity can be either:

- **Business organisation**, meaning a commercial private company;
- **Industry consortium** representing several industry players while having a non-commercial approach;
- **Public authority** standing for a government-driven approach in which the PKI is governed and managed by the public sector.

The interviews revealed that all the **single options – single business organisation, single industry consortium and single public authority – although avoid the complexity of having multiple PKIs**, these are subject to a **common security fault** known as a "**single point of failure**". In this case, the inability to operate of the single operating entity (i.e., technical issues, cyber threats, etc.) would **result in the whole PKI system coming into a halt**. Furthermore, in the case of a **single business organisation**, this could lead to a **monopoly** in the market. Similarly, the **single industry consortium** could be a viable option only if **large enough and representative of all the stakeholders in the market**, and if it would be structured to be open, non-profit and non-exclusive in order to ensure its correct functioning, representing all types of players within the markets; however, creating a consortium is not an easy matter due to, at times, diverging interests. The **single governmental agency** could successfully grant a fair, open and non-discriminatory access to PKI while promoting rules acceptance in the market and fair conflict resolution. The main downside of the latter, however, maybe it is requiring more time to **take action** at times due to the involvement of the government and bureaucracy, which may result in limitations especially when it comes to operating.

Multiple options

The multiple governance options prescribe **multiple entities governing and operating the PKI** that can be:

- **Business organisations**, meaning a combination of independent, commercial private companies;
- **Industry consortia**, each of them representing several industry players and having a non-commercial approach;
- **Public authorities** thus promoting government-driven approach in which the PKI is governed and managed by a combination of authorities from the public sector;

Among the multiple governance options there is one last alternative, the **mixed approach**. In this instance, the governance and operation of the PKI is executed by a **combination of entities coming from both the public and private sector**, thus involving businesses organisations, industry consortia, and one or more public authorities.

The interviews resulted in no PKI project developers and service providers backing up the governance by **multiple business organisations.** In fact, while the multiple options solve some of issues of its single counterpart, namely the risk of monopoly, there might be **issues linked to the private governance and issues of possible market fragmentation**. Additionally, the overall complexity would increase by the need of **establishing a task force or a working group to set up common rules and guarantee interoperability**. In the case of the **multiple industry consortia** option, while it may appear as the best choice when it comes to **impartiality**, **fairness**, and **openness**, the complexity of **setting up a board or working group to coordinate the members** would potentially result in **slow decision making**. Another issue might be related to the market fragmentation that could stem from the **conflict of interest linked to the pre-alliances** among the actors and the **business competition**. The **multiple Governmental Agencies** could be an acceptable option to grant a fair, open, and non-discriminatory access to PKI. In this **case, the number of agencies to be involved might vary in coordination with market development**. However, the involvement of multiple public authorities might amplify the issues highlighted for the single public authority option (e.g. doubling of functions, increased bureaucracy related to the involvement of multiple entities from the public sector, etc.). Hence, due to the nature of governmental operations, for this solution to work, a mechanism to ensure efficiency of operation (i.e., avoid **doubling of functions** or excessive **slowdowns due to bureaucracy**, etc.) needs to be in place.

Lastly, the consultation found the mixed approach - thus the **simultaneous involvement in the PKI governance of business organisation, industry consortia and the public sector** - as more suitable in ensuring the neutrality required to grant a fair, open and non-discriminatory access to PKI. Furthermore, **different entities can cover different governance roles**, thus allowing to **leverage the strengths of each category of entity and minimise the downsides**. Generally, the involvement of the public sector is predominantly associated with the criteria definition block, outlining the criteria for Root CAs to be considered trustable and defining the governance rules (i.e., auditing procedures), while the other two governance blocks (criteria conformance check, Trust List publishing if CTL applies) as well as functions linked to the operation of the PKI appear to be better suited to be covered by private actors (business organisations and industry consortia).

It is important to specify that the "**Mixed approach" governance is applicable to all governance models** listed in the paragraph above **(i.e. CTL, CC and CR)** by simply **assigning the roles** that they prescribe **to the different categories of actors**, in particular to the public sector, business organisations and industry consortia.

Conclusions on the PKI governance

When it comes to the governance model, a strong preference emerged (unanimous among the PKI projects of the STF sub-group) towards the **mixed approach**. The combination of all categories of entities – businesses organisation, industry consortia and public authorities – allows to **leverage the strengths of each of them while minimising the downsides**. Specifically, the **neutrality and acceptance of public authorities** can be deployed for high level governance roles, while the **flexibility and reactivity of the private sector** entities can be better suited for more operational roles. In addition, in the **governance of the PKI, there are a series of activities that have been identified and that need to be carried out**: the definition of a list of common criteria, compliance checking of the compliance of CAs against that set of criteria, and the publishing and management of the list of trusted CAs (applicable only in the CTL's case).

The **secondary legislation under AFIR could provide legal back-up to a detailed governance framework** which would be jointly defined by the European Commission and the STF sub-group, including the roles and responsibilities for each type of entity for the PKI governance and across the three governing blocks.

Recommendation 5: Ownership model

The fifth recommendation addresses the topic of the **ownership model of the e-mobility PKI**. **Building upon the conclusions of the previous recommendations**, which saw the governance mixed approach to be the preferred option, this recommendation further **explored the role of the public and private sectors** in the context of the PKI based on ISO 15118.

Analysis of the PKI ownership model

The ownership model of the PKI consists in **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 include the **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.

The roles are divided in the **two macro categories of (1) governing and (2) managing and operating, as described in Recommendation 4.** The full list of roles is presented in the image below.

Table 9: Identified list of PKI roles & responsibilities

Layer	Roles & responsibilities
Governing	Development of mutually recognized criteria to recognize Root CAs as trustworthy
	Setting up of rules and procedures to check criteria compliance of CAs
	Checking criteria compliance of CAs

Layer	Roles & responsibilities
	Licensing/Accreditation of CAs (only applicable to Cross-recognition)
	Monitoring of the governing bodies (e.g. Compliance authorities, CTL Manager, etc.)
	Definition of the requirements of the Certificate Policy and the Security Policy
	Guarantee interoperability for consumers
	Monitor PKIs and the fair, reasonable and non-discriminatory access to a PKI
	Monitor the interoperability process and its fair, reasonable and non-discriminatory access (i.e., access to the TLM, Licensing authorities, etc.)
	Publishing and managing of the list of trusted CAs
Managing and operating	Owning and operating V2G Root CAs
	Organize the acceptance of new V2G Root CAs
	Act as an intermediate in case of conflict and manage conflict filing and handling
	Interfaces definition and management

.

One of the aims of this recommendation, in synergy with the findings of recommendation 4, is understanding the actor better suited to cover each role and responsibility. As prescribed by the mixed approach (see paragraph 3.4.1) the possible alternatives are:

- **Business organisations**, which are characterised by **flexibility and agility** of operations, are **innovation-focused**, but as they are for-profit entities operating in the market, looking for competitive advantage over their competitors, they inherently lack neutrality and acceptance;
- **Industry consortia** provide **increased level of neutrality** as they represent a combination of market players albeit it is dependent on its composition (number and categories of players). It still **pertains some of the flexibility and innovation-driven approach** but has a **slower decision-making process** due to the discussion time that need to occur among members;
- **Public authorities** provide the **highest amount of neutrality and acceptance** as they do not hold any commercial interest in the market. This feature is counterbalanced by a **slower speed in the decision-making process** which is caused at times by the public sector's bureaucracy.

Conclusions on the PKI ownership model

Ownership of the governing layer

There is general consensus for a **public authority to perform the roles within the governing layer**. In particular the **involvement of the public sector was strongly suggested for the definition of the mutually recognised criteria to assess the Root CAs' trustworthiness**. Also, the preference was strongly oriented towards the public sector when it comes to activities such as **setting up roles and procedures to check the criteria compliance** (i.e., auditing procedures), **definition of the requirements of the Certificate Policy and Security Policy**. In addition to that, only an entity such as a public authority can **guarantee interoperability for consumers**, **monitor the fair, open, and non-discriminatory access to PKI and to the interoperability solution of choice**.

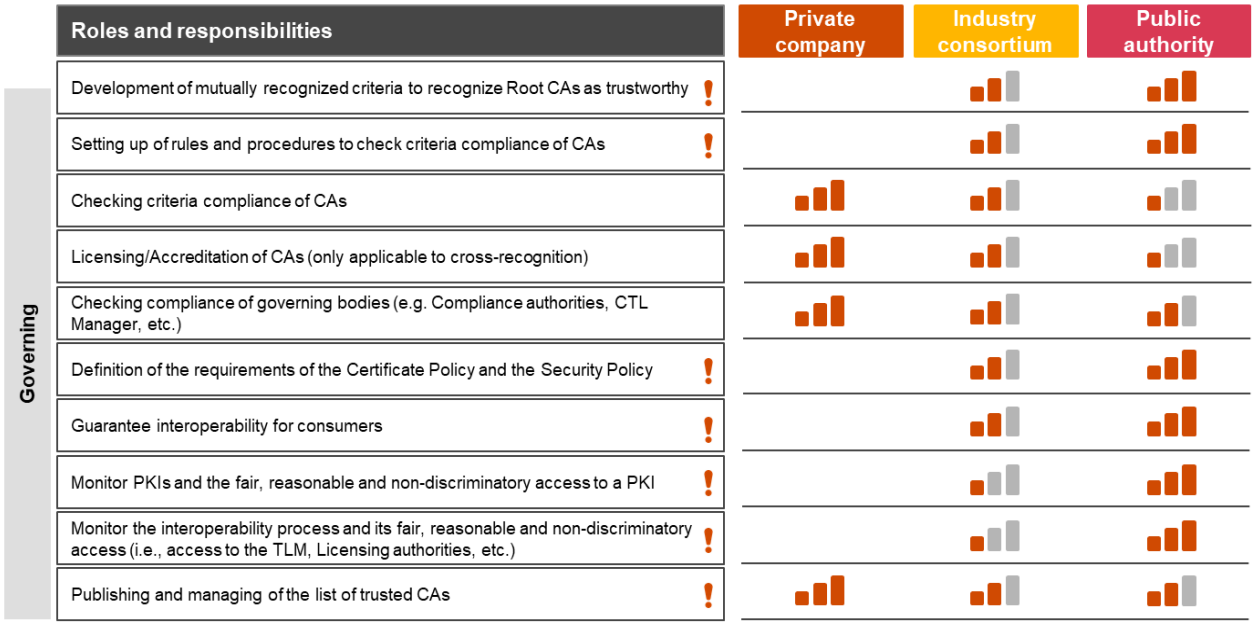
In particular, among the type of public authorities available, the preference was for the **European Commission** to cover such role because it can guarantee **higher impartiality and acceptance** which is of outmost impotence for the governance of a PKI, and especially for the first governance block.

All the governing roles mentioned up to this point might also be covered by an industry Consortium bringing advantages linked to the agility and adaptability at the expenses of overall impartiality and acceptance in the market. **However, the composition of the industry consortium in charge of fundamental governing roles can be critical and problematic under several perspectives**. First, the consortium **should be large enough to provide adequate representation of the different perspectives in the market**. Secondly, it **should be representative of all categories of market players** containing a balanced representation of OEMs, CPOs, and EMSPs among many others. This brings an additional layer of complexity. As the e-mobility PKI evolves with new and, to date, unpredictable features, **the boundaries of the actors than need to be represented in the said consortium grows larger**. A simple example is the smart charging features that would require players from the energy sector such as DSOs to be represented as well. As a consequence, the **Consortium composition** would be subject to **continuous expansion**, meaning **the representation of actors would need to be regularly reviewed** rendering the consortium **extremely complex to manage and to ensure the neutrality required** for the high-level governance.

At governing level there are **three roles which, due to their nature, are better suited to be covered by the private companies** under the rules set up by the governing authority. Specifically, **checking the criteria compliance** of V2G Root CAs, the **licensing/accreditation** of the same entities, as well as **checking the compliance of governing bodies** to the rules and procedures outlined by the neutral and accepted governing authority. These **compliance checking roles, such as auditing, are in business practice generally efficiently performed by private companies such as accredited PKI auditors**.

The preference of the PKI project developers and service providers of the STF Sub-group on G&S on the ownership of the governing layer is reflected in the image below.

Figure 7: PKI project developers and service providers' preferences on ownership of the governing layer



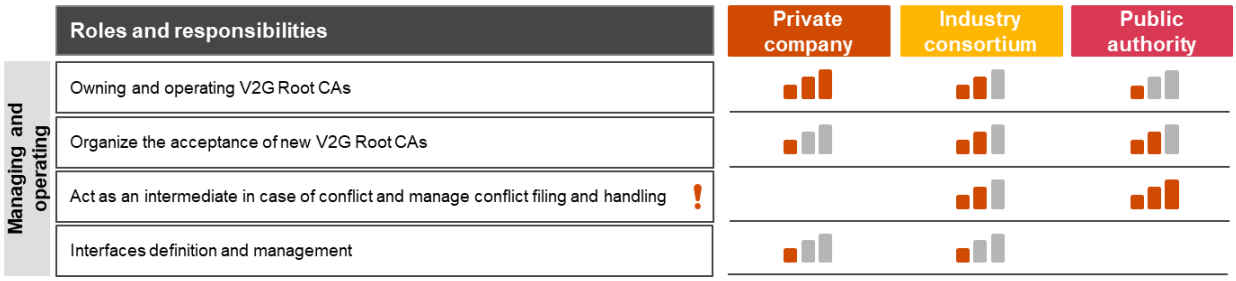
Please note, the roles that should be addressed by only one of the actors' categories are marked with an exclamation mark.

Ownership of the managing and operating layer

As for the governing layer, the managing and operating layer could be covered by a combination of business organisations, industry consortia and public authorities. For the roles and responsibilities under the managing and operating layer there is a **higher level of flexibility** for the entities covering them. The **ownership and operation of V2G Root CAs can be performed by all categories**, with private companies being the most preferred, followed by industry consortia. The presence of a publicly owned Root CAs is seen as optional. The order of preference is reversed when it comes to organising the **acceptance of new Root CAs**, as more neutral and accepted authority can mediate with the market in a more effective way. Similarly the **public sector was favoured in being assigned the responsibility of acting as an intermediate in case of conflict and manage conflict filing and handling**. The only possible alternative for this task could be a large industry consortium due to the broad level of accountability. Lastly, both private companies and consortia could be responsible for **interface definition and management**.

The preference of the PKI project developers and service providers of the STF Sub-group on G&S is reflected in the image below.

Figure 8: PKI project provider's preferences on ownership of the managing and operating layer



Please note, the roles that should be addressed by only **one of the actors' categories** are marked with an exclamation mark.

Concluding remarks on Recommendation 5

The fifth recommendation built upon the emerged preference towards the mixed approach to the governance of the PKI, expanding on the roles that the different categories of entities are better suited to cover. In particular, it emerged that the **public sector should be in charge of the governing layer of** the PKI (i.e., definition of governance rules and criteria for CAs trustworthiness), while the **businesses organisations and industry consortia should be mainly responsible of managing and operating the PKI** (i.e., owning V2G Root CAs, criteria compliance check, etc.).

In addition, in recommendation 5 the topics of **transparency in operating V2G Root** CAs and **mechanisms to ensure a fair, open, and non-discriminatory access to the PKI** were also covered. The former can be addressed in the secondary legislation by the setup of **technical requirements** (i.e., publication of CP and SP based on a set of minimum criteria) in conjunction with the backup in the regulation of **market rules** focussing on **security and scalability**. To ensure a fair, open, non-discriminatory access to the PKI the main identified mechanisms are:

- **Avoiding users lock-in effect** by ensuring seamless data portability when switching among PKI operators;
- Defining **access conditions** to other PKIs by identifying the trusted actors;
- Definition and **adoption of common APIs and protocols**.

In addition to this, for recommendation 5, PwC addressed additional aspects related to the ownership of the PKI.

In particular, PwC deep dived on:

- the **organisational requirements** and legal obligation of the main actors in the PKI system;
- **criteria to ensure transparency** and a level playing field in the e-mobility PKI ecosystem;
- **financing of the governing layer** of the PKI.

The table below provides a description of the characteristics that, according to the PKI project developers and service providers consulted, the actors of the PKY ecosystem should have.

Table 10: Additional aspects related to ownership

Additional ownership aspects	Description
Organisational requirement and legal obligations for the identified minimum set of actors required to ensure a functioning PKI ecosystem	This includes: • The **body responsible for the definition of the criteria** to consider V2G Root CAs as trustworthy; • **Compliance checking bodies**, defined as all the entities which will be responsible to check whether the CAs abide to the established criteria to be considered trustworthy; • **Trust List Manager** if the CTL is the preferred interoperability option; • **Licensing/accreditation bodies** if the Cross-recognition is the applied interoperability option. When it comes to the licensing/accreditation body, the most important requirement is for it to be a **neutral and widely accepted**, characteristics that can be granted only by a **non-profit industry wide-consortium or a public authority**. Among the required legal obligations for this entity, there are **fairness, openness, non-discriminatory behaviours**, and the ability to **represent all PKI actors within the ecosystem**. The **Compliance checking bodies and the licensing/accreditation** bodies have similar requirements. They should be **required to have declaration/certificate listing their conformity against a series of requirements** by the body in charge of the governance. In addition they can be **for-profit**. Being **open and non-discriminatory** is their common legal obligation, as well as the obligation to **follow the compliance checking process set up by the regulator** for the compliance checking bodies. Lastly the **TLM** is required to be **non-profit** and **operated under responsibility of a public authority or cross-industry consortium** recognized by the whole ecosystem. For these actors there are several legal obligations, which include **Publishing of the content of the CTL at service level**, being **monitored by a public authority**, being **open and non-discriminatory**, reliable, proven, and trustful, have **transparency on rules**. In general, **organisations covering roles at governing level should be non-profit and certify their conformity against a set of requirements**. In terms of legal obligations, they should be **open and non-discriminatory** towards the other actors within the PKI ecosystem. At **managing and operating level** it included V2G Root CAs and PKI pool operator which support V2G Root CA offering Central Contract Certificate Pools and central OEM Provisioning Certificate Pools. For both of those actors the identified organisational requirement is to be **highly trustable organisations**. V2G Root CAs main legal obligations is **publishing the CP and Certificate Practice statement** and **compliant with minimum set of criteria defined for trustworthiness of CAs**, followed by not adopting discriminatory behaviours and being compliant with **competition rules to prevent abuse of dominant position** in the market. **Non-discriminatory behaviours apply to PKI pool operators as well, in addition to fair pricing**.
Criteria to ensure transparency from the organisations operating a V2G Root CA as well as to ensure a fair, open, and non-discriminatory access to PKIs.	These are: 1. **Transparency in operating V2G Root Cas:** The operation of V2G Root CAs is one of the most important roles in the e-mobility PKI ecosystem due to being at the top of the **hierarchy of the certificate emission and signing**. Thus, transparency in operations is of particular importance. From the consultation, it emerged that the inclusion of a **minimum set of requirements** in conjunction with the **publication of Certificate and Security Policies** are the most important steps to ensure transparency. Additional mechanisms relate to the accessibility for all customers to the **Certificate Practice Statement** (CPS), a providing clear **cost construction** of the service, as well as overall **clarity on data usage**. 2. **Fair, open, and non-discriminatory access to PKIs: Ensuring fair, open, and non-discriminatory access to PKIs to consumer is paramount**, especially in a multi V2G

	Root CA model. The main mechanisms to achieve this purpose **is avoiding the customers' lock in effect** by establishing data portability and thus a **seamless transition among different PKI operators**. Ancillary to that would be, the **definition for common Application Programming Interfaces** (APIs), the definition of the **access condition to PKIs**, and of the **set of trusted actors** that are accepted in the PKI ecosystem.
Financing the governance layer	As mentioned, the high-level governance of the PKI is better suited to be covered by a neutral and accepted authority. Specifically it can either be a public authority (i.e., the European Commission or a delegate) or and industry consortia. Recommendation 5 covered the topic of financing the governing layer of the e-mobility PKI considering both options. The governance by an **industry consortium** would be financed though **participation fees** contributed by the members of the consortium. In case of the governance by a public authority two routes are possible. The first one foresees the **exclusive use of public funding** (i.e., CEF). The second prescribes a **cost-covering fee** (i.e., tax) applied to participants in the PKI. In this case the following elements need to be taken into account: • The **subjects to which the fee** is applied need to be defined in a **fair and clear way**; • The **time of payment** needs to be defined; • The possible repercussion of the cost-covering fee the deployment of Plug&Charge.

Recommendation 6: Implementation scheme for the proposed governance and architecture solution

Recommendation 6 – which looks at the implementation scheme for the proposed governance and architecture - was the last recommendation addressed by PwC in the first phase of the Support Study. The primary aim of this round of consultations was to assess the **readiness of governance, policies & standards and technical specifications for the different interoperability options**. The second was to **define an implementation roadmap** covering the initial implementation and the full implementation phases addressing the timing, activities and risks.

Analysis of the PKI implementation scheme - Implementation readiness assessment

Under specific suggestion of the JRC as operator of the C-ITS, the following variables were used to assess the readiness of the interoperability options: **governance**, **policies & standards** and **technical specifications**. It was explored whether these aspects were already available and in place or if they still need to be developed in relation to each of the interoperability options. These aspects in fact, were critical in the development of the C-ITS system and slowed down the overall implementation when their readiness was lacking. In order to avoid those shortcomings, assessing the readiness of each interoperability option is crucial as it should support in understanding which are the elements that still need to be developed to have a smooth implementation in latter stages.

The interviews found the **Cross-certification** to be the interoperability option with the **highest implementation readiness**.

In terms of **governance**, and **policy & standards,** these were consistent among the interoperability options. In fact, regardless of the solution implemented, there is a need to:

- Define criteria for determine the trustworthiness of V2G root CAs;

- Define an audit process;
- Develop roles, controls, conditions and rules.

The PKI project developers and service providers however, identified **Cross-certification** as **ready under the technical specification** point of view. The cause of this advantage, according to the PKI project developers and service providers, is dependant of the extensive testing which this solution has experienced as well as its nature based on bilateral agreements among actors.

Cross-recognition resulted as **partially ready for implementation**. Similarly to Cross-certification, it is reliant upon negotiation and agreements among PKI operators but for it to be implemented it would require a more intensive ecosystem organisation and market rules (i.e., the agreement among Root CAs, for this please refer to paragraph 3.3.1.2).

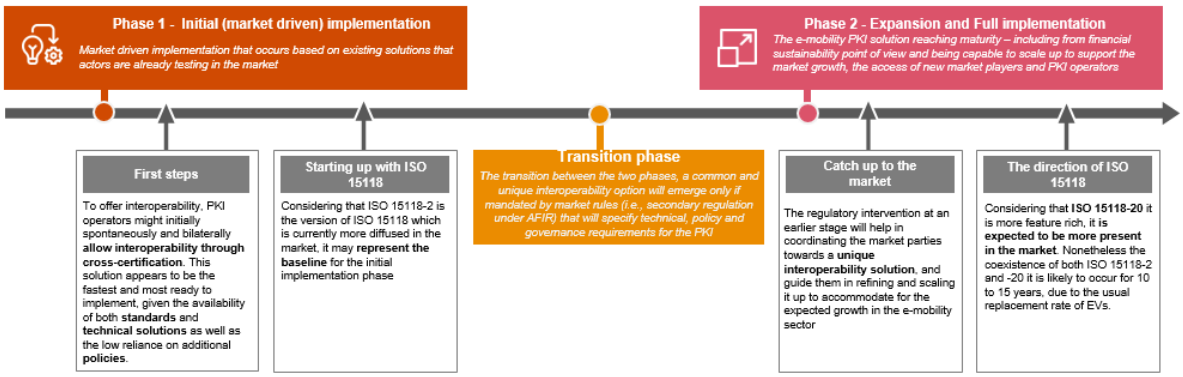
The **CTL** is also **partially ready for implementation**, although it may lag behind the other solutions in terms of overall implementation readiness. This is partly due to the CTL's top-down centralised approach which arguably cause it to be more reliant on governance, policies and standards. As mentioned before in fact, while policies and standards are consistent for all interoperability solution, considering the crucial role that they cover for the implementation of the CTL it decreases its implementation readiness. When it comes to **technical solutions**, the CTL has the status of being partially ready as it only adds external modules aimed at managing the trust store, but still some additional work to achieve a **more comprehensive standardisation of interfaces is needed**. The CTL, however, can catch up with the readiness level of the other solutions by leveraging on the numerous and relevant best practices present in other industries, especially the C-ITS which is the reference practice for PKIs through the use of CTL.

Conclusions on the PKI implementation scheme - Implementation roadmap

The consultations allowed the development of an implementation roadmap which **outlines the expected development path of the EU PKI ecosystem**. The roadmap is articulated in two phases, with a transition period in between:

A. Initial implementation of the PKI ecosystem, **marked-driven phase** characterised by the isolated PKI systems by market operators and potential interoperability solutions brought to the market if demand increases and time-to-market feasible;
B. **Transition phase** in which the preferred EU PKI governance and architecture will emerge only, supported by regulation (i.e., secondary regulation under AFIR);
C. Expansion and full implementation of the EU PKI ecosystem, facilitated by the secondary legislation that would promote the adoption of a **common and unique interoperability solution (i.e., CTL)** in the market driven by clear **market rules and EU legal provisions**. Set-up and technical CTL implementation by a public organisation (i.e., JRC) in cooperation with the private sector (i.e., industry stakeholders).

Figure 9: Implementation roadmap



1) Initial (market driven) implementation

The first phase, the initial implementation of the PKI, is expected to be **characterised by existing solutions** which are being tested thoroughly by actors in the market. In accordance with Recommendation 3, in this phase a potential individual PKI system will offer services, and, eventually, market actors would implement some type of **interoperability solution**. This solution is however not expected to scale up, given the potential establishment in EU legislation of a common EU solution based on a preferred interoperability approach.

A possibility, although unlikely due to time-to-market and upcoming AFIR delegated act, is that some **PKI service providers spontaneously and bilaterally offer interoperability through Cross-Certification**, as it seems the solution with the highest readiness (or easier to implement in short time). Due to it being the fastest solution to implement, Cross-certification could also be a **temporary solution** that the market players **set up for a limited period of time** until **it is replaced by another preferred solution, once it is ready** (i.e., CTL). Regardless of the implementation approach, this phase would have to be based on ISO 15118-2 as it is currently the most common version in the market and is already embedded in the majority on devices.

Furthermore, should **Cross-certification and Cross-recognition be initially implemented**, the main activities will be centred around strong negotiation efforts among the PKI operators to reach the agreements necessary for the functioning of the solutions. In addition, **Cross-certification** would require the definition of the solution for the technical signature across actors, and the definition of technical interfaces for charging stations. **Cross-recognition**, instead, would require the definition of a method to update the certificates embedded in EVs and CSs at the entry of new PKI actors in the market. The **implementation timing** of these two interoperability options is subject to a high degree of variance as it would heavily depend on the negotiation timing among the market actors. Additionally, the **main risk** that both solutions impose regard the **scale-up process**. Specifically, Cross-recognition Cross-certification might not be able to sustain the expected e-mobility market expansion. Furthermore, Cross-certification could be associated with three additional exposures. First, it might require timely regulatory support to avoid the partial-mash issue (see section 3.3.1). Secondly, if the two-step implementation process is chosen, there is the concrete risk that the temporary solution, and specifically Cross-certification, might remain in the market even after the adoption of the CTL. Third, the EU regulator decision on a common approach for EU PKI interoperability would put out of the market other solutions, brought exclusively by some market actors without a whole public-private consensus.

The implementation of the **CTL, on the other hand, requires several activities**. The first and more relevant, regards the **selection of the actor responsible for the governance of CTL** and of the operative actor covering the **role of Trust List Manager**. Then the **technical set up** of the CTL would need to be addressed together with the definition of clear APIs and interfaces. Furthermore, the procedures to be included and removed by the list would need to be clearly defined. In conjunction, in order to have a functioning PKI based on the CTL, it would need to be integrated in all the end-devices (EVs, EVSEs, etc.). When it comes to **timing**, the CTL managed by a public authority will most likely require **one year to be implemented**, **starting from the executive decision** mandating its adoption. Thus, the concrete implementation timing would need to take into account for the **additional time needed to come to the said executive decision**. Under the **risk perspective**, the CTL is associated with a larger financial and workload investment when compared to the other two options, however, this cost would be centralised as it would be borne mainly by the Trust List Manager and the entity responsible for the governance of the CTL.

2) Transition phase

Between the two phases, there will be a transition phase where **regulation will have a primary role**. This is due to the fact that regulation represents a crucial step to **ensure interoperability to consumers** as well as in **supporting the growth of the market**. In addition, the early emergence of a common and unique interoperability solution would be strongly dependant on the presence of formal rules mandating it (i.e., secondary regulation under AFIR). Lastly the regulation would facilitate implementation by including a **minimum set of technical specifications**, as well as **defining policies and governance requirements**.

3) Expansion and full implementation

The full implementation phase consists in the chosen interoperability option (i.e., CTL – Recommendation 3) **reaching maturity to support the expansion of the e-mobility market**. This assumes particular relevance considering the bivalent nature of the expected market development. On the one side, the e-mobility market is expected to experience a **rapid adoption of EVs**. As a consequence, the e-mobility market players - PKI operators but also EMSPs, CPOs, etc. - are expected to face a similar growth in both size and number to accommodate the increase in demand of their services.

The **CTL does not become more complex with the two-folded growth of the market** and is able to maintain **lower and centralised operational costs** and efforts in time. In addition, the CTL has a greater potential to create interoperability with sectors and markets related to e-mobility.

The **activities necessary for the scaling up** of the preferred interoperability solution – CTL - are the **definition and adoption of a number of minimum technical requirements**, **governance and architecture aspects[16] and technical specifications (i.e., standards)**, that would enable the **wide implementation of EU PKI ecosystem, firstly in this case for Plug&Charge**.

[16] Particularly, the full implementation of the CTL would be accompanied by the incorporation of certificate pools.

Cost estimation of the governance and architecture preferred option - CTL

As part of the study, a number of consultations were carried out with the European Commission and the Joint Research Centre (JRC) on the **potential costs and financial sustainability** concerning the public set-up and implementation of a EU PKI ecosystem for e-mobility.

Considering other reference projects, such as the C-ITS based also on CTL architecture and implemented by the JRC, it was possible to conclude a **CAPEX estimation** of approximately **EUR 1 M** to **initially set-up and put into functioning the PKI for e-mobility based on a CTL** interoperable architecture and in line with all the technical requirements further elaborated in Phase 2 of this study. In addition, it was also concluded an **OPEX** of approximately **EUR 500,000** to **maintain the system running every year**. It is possible that these costs estimated could be further reduced depending on the possibility of potential reutilization of existing CTL systems used by JRC as part of the C-ITS project.

The future financing of a public authority (e.g., European Commission) to carry out the roles of this governance and architecture 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. If the European Commission may consider necessary applying a tax, the subjects to which the fee is applied would need to be defined in a fair and clear way. The European Commission as public authority should address this matter in discussion with industry participants in order to determine the amount of that cost-covering fee.

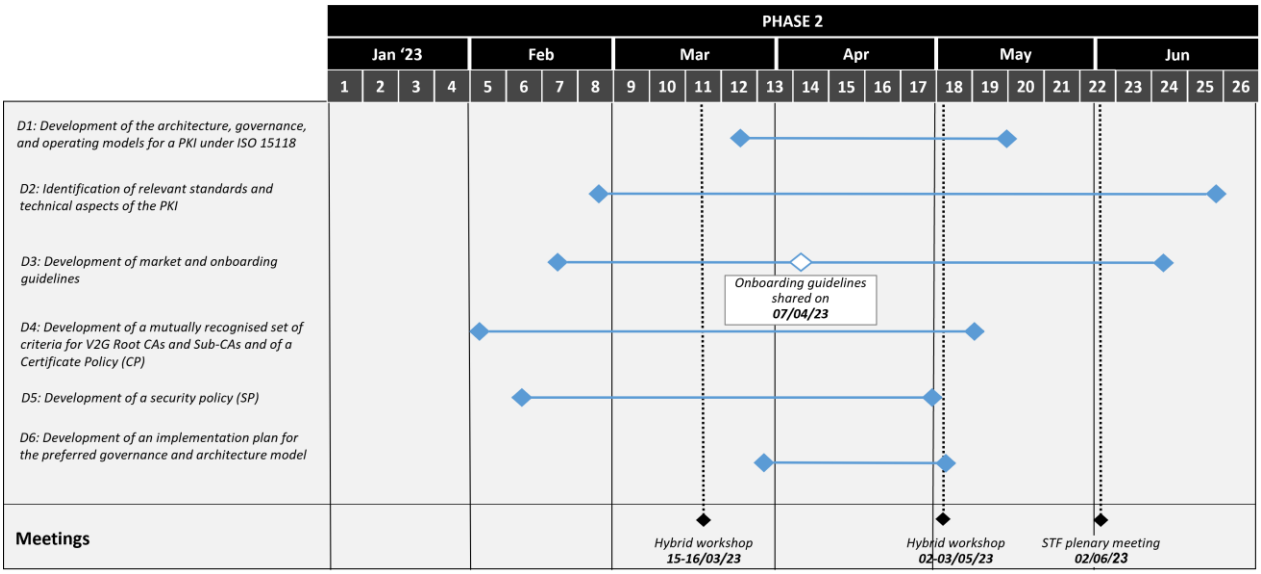
3 Phase 2 – Definition of technical and policy specifications

3.1 Methodology for Phase 2 of the Support Study

The second phase of the study ran from the end of January 2023 to the end of June 2023. It aimed at **building upon the first phase of the Support Study**, by de**lving deeper into the identified areas** that needed to be developed for the secondary legislation under AFIR. In order to do so, PwC in collaboration with DG MOVE created a **dedicated working group** of experts that worked collaboratively on the set of deliverables later described.

The following Gantt chart shows the timeline for the deliverables and meetings of Phase 2.

Figure 10: Gantt chart of the second phase of the study



In the following paragraphs we describe the methodology in further detail.

Identification of the deliverables

As the first step in Phase 2 of the study, the **set of topics to focus on in the second part of the Support Study** were identified.

The starting point for the analysis was the **information collected throughout the different round of interviews** carried in the first phase of the assignment, **desk research**, as well as looking at **best practices** and the **available publications**. This included the consultation of several industry papers (i.e. ElaadNL's PKI for ISO 15118[17], AFIREV's Recommendation on communication security for roaming electric vehicle charging[18], CharIN Position Paper of Charging Interface Initiative e.V[19], etc.).

However, **the main driver** for pinpointing the topics - which would have then become the focus of the deliverables of the second phase of the study - was the identification of **best practices already implemented in Europe sharing the fundamental PKI characteristics** emerged from phase 1. Among the available best practices, the **Cooperative Intelligent Transport System** (C-TS) operated by the Joint Research Centre of the European Commission was the most suitable one to act as the main reference practice. As a matter of fact, the C-ITS's PKI has:

- A **regulated approach** (Recommendation 1);
- A **multi-Root CA model** (Recommendation 2);
- The **CTL** as chosen solution to reach interoperability (Recommendation 3);
- A **mixed approach to PKI governance** (Recommendation 4);

[17] Source : https://elaad.nl/wp-content/uploads/downloads/PKI-for-ISO-15118-2022-pdf.pdf
[18] Source : https://www.afirev.fr/wp-content/uploads/2019/11/AFIREV_Reco_PKI_ISO15118_2019-En.pdf
[19] Source : https://www.charin.global/media/pages/technology/knowledge-base/8ec83b4f9c-1615552576/190520_charin_one_page_information_displayed_on_charging_stations_v2.2.pdf

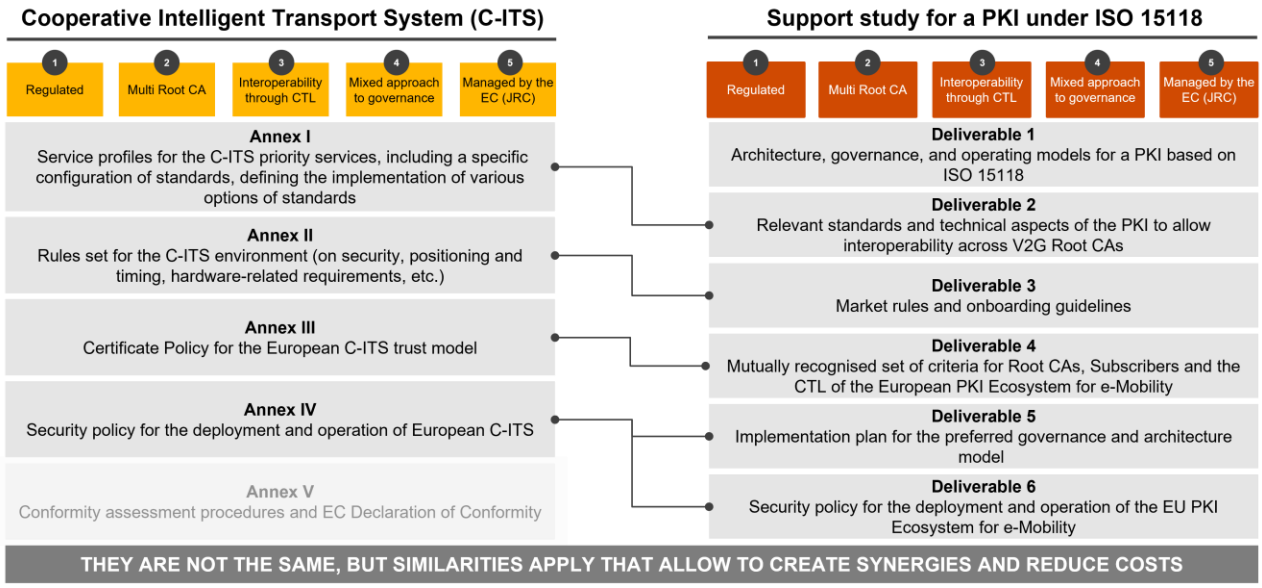
- The **European Commission**, and specifically the JRC, covering the **governance and management** of the PKI (Recommendation 5).

As a consequence, the C-ITS's delegated acts[20] have been the main source used to identify the deliverables to develop during Phase 2. Specifically the deliverables developed in the second phase of the study are:

- **Deliverable 1** - **Architecture, governance, and operating model** for a PKI based on ISO 15118;
- **Deliverable 2** - **Relevant standards and technical aspects** of the PKI to allow interoperability across V2G Root CAs;
- **Deliverable 3** - **Market rules** for the EU PKI ecosystem for e-mobility;
- **Deliverable 4** - **Mutually recognised set of criteria** for Root CAs, Subscribers and the CTL of the EU PKI ecosystem for e-mobility;
- **Deliverable 5** - **Implementation plan** for the preferred governance and architecture model;
- **Deliverable 6** - **Security policy** for the deployment and operation of the EU PKI ecosystem for e-Mobility.

The image below offers a comparison between the six deliverables of the Support Study and the Annexes to the C-ITS delegated acts.

Figure 11: Comparison with the reference practice of C-ITS



[20] Source : https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1381-Specifications-for-the-provision-of-cooperative-intelligent-transport-systems-C-ITS-_en

Establishment of a Working Group (WG)

On the 16th of January, in the occasion of the first STF Sub-group on G&S meeting of 2023, the STF Sub-group members were informed of the creation of a working group and **any interested party** was invited to **express their willingness to join this group** by the 23rd of January.

Most notably, the group included of PKI project developers and service providers, the members of Activity 2 – Block 3, and the JRC. The table below list the organisations that joined the working group.

Table 11: Organisations taking part in the working group

#	Representatives	Representatives
1	ChargePoint, SAE, EV Roaming Foundation and ChargeUp Europe	Kor Meelker
2	CharIN	Christoph Albrecht
3	CharIN	Glenn Cezanne
4	CharIN	Kjeld B. Olesen
5	CharIN	Michael Keller
6	DG MOVE	Saki Gerassis Davite
7	DG MOVE	Antonio Tricas
8	e-clearing.net	Aya Muhammad
9	ElaadNL	Baerte de Brey
10	ElaadNL	Lonneke Driessen
11	Elli	Matthias Foerth
12	EnBW	Scheubner Stefan
13	Gireve	Jean-Marc Rives
14	Gireve	Margaux Vandeville
15	Hubject	Christian Hahn
16	JRC	Antonio Herrera Alcantara
17	JRC	Silvia Capato
18	PwC	Enrico Gaspari
19	PwC	Vivian Leamy
20	PwC	Andrea De Angelis
21	Shell	Karl Weinreich
22	Shell	Sebastian Vetterlein
23	Smartlab gmbh	Moritz Dickehage
24	Tesla	Mattheo van der Molen
25	Vedecom	Mourad Tiguercha

The **participation in the working group was on a voluntary basis**. However, WG members were asked to respect a list of requirements to ensure the successful outcome of the working group meetings:

1. Participants should provide **relevant technical expertise** for the WG;
2. Participants should be entitled to **take position and decisions** on the topics discussed during the meetings;
3. Participants should **contribute actively and constructively** and **provide inputs and feedback**;
4. Participants should **facilitate collaboration** and **exchange of information**;
5. Participants should allow for **agenda flexibility** and **availability**.

In total the group was constituted by **24 stakeholders** and industry representatives and encapsulated the perspective of **14 market players** (not counting DG MOVE, JRC, and PwC).

Consultation methods

To produce and validate the deliverables, **three kinds of consultation methods** were deployed. The table below summarises the list of consultation activities that were carried out in the second part of the study, starting from January 2023.

Table 12: Consultation tools

Tool	Description	Potential targets	Timing	Output
Weekly Working Group Meetings	Elaboration, discussion and review of the six deliverables	All working group members	On a weekly basis from February '23 - June '23	• Deliverables
Hybrid Workshops	Speed up the content production of the deliverables, revise and comment the deliverables, gather feedback on the already developed topics and validate the next steps of the assignment	All working group members	15-16 March '23, 02-03 May '23	• Deliverables • Feedback and insight collection • Validation of developed topics • Validation of subsequent steps of the study
STF recurring meetings	Recurring meetings of the STF sub-group aimed at updating on the progress of the Support Study and collect insights and feedback	STF sub-group	On a monthly basis from February '23 - July '23	• Feedback and insight collection • Validation of developed topics • Validation of subsequent steps of the study
STF final validation Workshop	Gather feedback from members of the STF sub-group and validate the deliverables	STF sub-group	June 2nd 2023	• Feedback and insight collection • Validation of deliverables

In addition to these, **several progress meetings** have been organised with the **European Commission** and the **JRC** to **oversee the progress of the working group**, discuss strategic topics of the assignment and provide an update on the work carried out and the content developed. This process ensured that the direction taken by the working group was shared by the European Commission, the content being produced was relevant and of high-quality. Additionally, those meetings served the purpose of st**eering the study and to take corrective actions**, if needed.

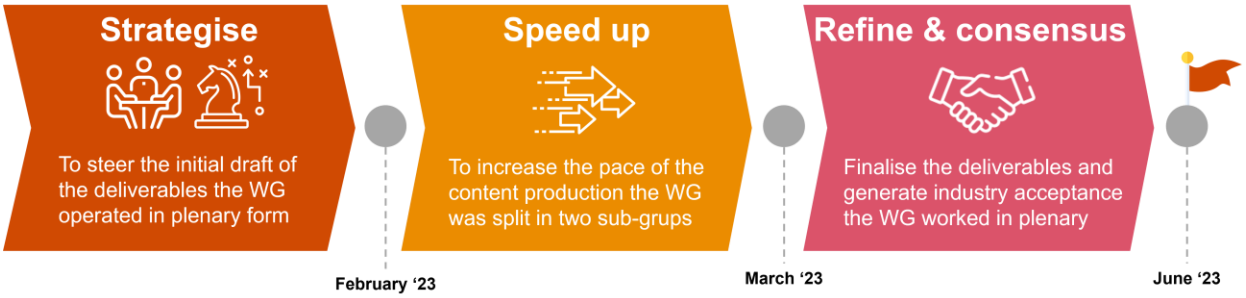
Weekly Working Group Meetings

The **working group** (WG) met virtually for weekly **two-hour sessions** from **February to June 2023**. The working group meetings were the primary tool for the **development of the six deliverables**.

Starting from a **draft of each deliverable provided by PwC**, the working group members revised the documents to **provide feedback** and contribute to the content creation during the meeting. During the meetings, PwC animated the **group discussion** to address the key aspects of the deliverables.

The work of the WG followed the flow outlined in the image below.

Figure 12: WG workflow



For the first month, the WG meetings consisted in plenary sessions. This was done with the purpose of **jumpstarting the deliverables and steer the initial content creation** by understanding what the needs were for each deliverable.

From February to March '23, after the first hybrid workshop (15-16 Mar. '23), the **working group was split into two separate sub-groups** that run separately and simultaneously up to the second hybrid workshop (2-3 May '23). **Each sub-group was in charge of different deliverables**. This was done with the purpose of **maximising the efficiency and effectiveness of the content creation** once a clear path forward was established in the previous stage. The sub-groups met regularly in plenary sessions to review the work done by the sub-group and validate it. The two sub-groups and their respective deliverables are represented in the table below.

Table 13: WG participants division

WG Sub-group 1	WG Sub-group 2
• **Deliverable 1** - Architecture, governance, and operating models for a PKI based on ISO 1511; • **Deliverable 4** – Mutually recognised set of criteria for Root CAs, Subscribers and the CTL of the EU PKI ecosystem for e-mobility; • **Deliverable 6** - Security policy for the deployment and operation of the EU PKI ecosystem for e-mobility.	• **Deliverable 2** - Relevant standards and technical aspects of the PKI to allow interoperability across Root CAs; • **Deliverable 3** - Market rules for the EU PKI ecosystem for e-mobility.
CharIN - Glenn Cezanne	ChargePoint - Kor Meelker
CharIN - Kjeld B. Olesen	DG MOVE - Saki Gerassis
Gireve - Vandeville Margaux	E-clearing.net - Aya Muhammad

Hubject - Christian Hahn	Enbw - Scheubner Stefan
JRC - Antonio Herrera Alcantara	PwC - Enrico Gaspari
PwC - Andrea De Angelis	Shell - Karl Weinreich
Vedecom - Tiguercha Mourad	Smartlab gmbh - Moritz Dickehage
	Tesla - Mattheo van der Molen

From May ’23 onward, the working group meeting proceeded in **plenary form only**. This was done as most deliverables reached sufficient progress or were drafted entirely and there was a need to **validate the content produced by the separate sub-groups**. In this stage in fact, the aim was to **collect feedback** and **generate consensus** in the whole group to **refine the deliverables** as well as **promoting their acceptance** in the industry.

Hybrid workshops

In accordance with the Commission, two workshop were organised with working group members with the purpose of **speeding up the content production for the deliverables**, gathering feedback and discussing the next steps of the study.

Both workshops had a **two-day duration** and were organised in a **hybrid format** allowing for in-presence participation in a selected European Commission’s premise in Brussels or online participation using a teleconferencing tool (e.g., Google Meet, Webex, etc). The **fist workshop** was held on **15-16th March ’23** and acted as an **intermediate milestone** in the development of the deliverables. The **second one** was organised on **02-03 May 2023** and aimed at **finalising the deliverables** from **a content perspective** prior to the final validation workshop.

STF recurring meetings

The STF recurring meeting were held on a monthly basis form February ’23 to July ’23. These meetings were used to **progressively present to the STF sub-group on G&S updates** on the Support Study and collect **insights and feedback**. Additionally, they were also used to **validate** the fundamental contents of the Study (e.g., governance and architecture of the EU PKI ecosystem for e-mobility) and to **steer the subsequent steps**.

STF final validation workshop

The aim of the **STF Plenary meeting** on 02nd June 2023 was to collect the **final round of feedback and validate the six deliverables**. Specifically, prior to the meeting PwC shared the deliverables with the STF requesting feedback in order to process it in time for the assembly. Then, during the meeting PwC presented to the STF a summary of the whole journey of the study and the key aspects of the deliverables. By doing so, it was possible to reach the approval from the STF for the deliverables as they are annexed to this document.

3.2 Results of Phase 2

The focus of the second phase of the study was to initially **develop six in-depth deliverables** concerning important aspects in **support of the preparation of the secondary legislation** (i.e.

delegated and/or implementing acts) **under the Alternative Fuels Infrastructure Regulation** (AFIR)[21] concerning the **set up and operation of the EU PKI ecosystem for e-mobility**. Those aspects were identified thanks to the results of the **first phase of the study**, which highlighted the main characteristics of the European PKI ecosystem, then deepened through **desk research** and the establishment of the working group (see 3.1).

At the moment of finalising this Support Study, the deliverables developed at working level were finally reordered in order to provide a clear conceptual explanation in a sequential form as part of this final report. Finally, a total 5 deliverables were completed and are part of this final report and Annex as follows:

- Deliverable 1 - Architecture, governance, and operating model for a PKI based on ISO 15118;
- Deliverable 2 - Relevant standards and technical aspects of the PKI to allow interoperability across V2G Root CAs;
- Deliverable 3 - Market rules for the EU PKI ecosystem for e-mobility;
- Deliverable 4 - Mutually recognised set of criteria for Root CAs, Subscribers and the CTL of the EU PKI ecosystem for e-mobility;
- Deliverable 5 - Implementation plan for the preferred governance and architecture model;

A number of concrete outstanding elements (i.e., minimum requirements for Certificate and Security Policy and Onboarding Guidelines), which were initially part of the deliverables envisaged in Phase 2, are not included in this final report and annex, due to the need to perform some further developments and fine-tuning. These outstanding elements, some in advance state of development, are in draft form at disposal of the European Commission and participant members of the working group. PwC advises to the European Commission to finalise these pending aspects with a dedicated group of experts as in Phase 2 of this Support Study.

The paragraphs below provide a breakdown of the deliverables summarising their most relevant aspects. All relevant materials of the deliverables are included in the Annex to this Support Study.

Phase 2 Deliverables

Deliverable 1 - Architecture, governance, and operating model for a PKI based on ISO 15118

In the context of the Support Study, **Deliverable 1** conceptualises the **governance and architecture framework of the EU PKI ecosystem for e-mobility**. This document outlines the concrete governance and architecture conditions, the **roles and responsibilities** of the different bodies within EU PKI ecosystem as well as between the EU PKI ecosystem and the multiple PKI systems operating in the market.

Firstly, the deliverable gathers the **main definitions applicable to the entire Support Study** and, subsequently, to all the relevant documents and materials produced (e.g., certificate and

[21] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1867

security policies, market rules, technical specifications, etc.). Here, the **clear differentiation between EU PKI ecosystem and PKI system** is critical for a sound understanding of the whole governance and architecture approach in the EU. The harmonisation of definitions by industry actors in alignment with the EU legislator is essential to put in place a regulated approach that effectively supports market actors and facilitates the development of a **level playing field backed-up by EU legislation**, capable also of endorsing other use cases including those that might arise in the future.

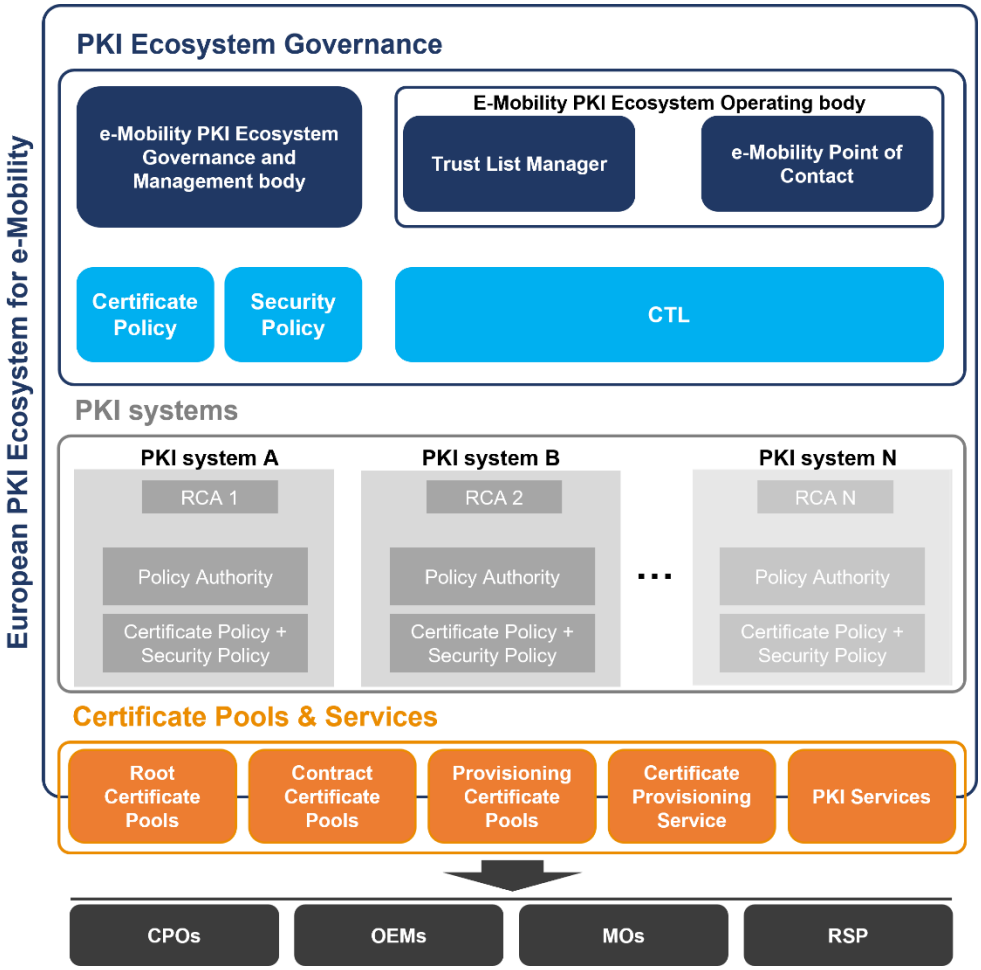
Secondly, the document elaborates the **main governance bodies and architecture elements** for the set-up and operation of a EU PKI ecosystem according to the high-level criteria previously defined (Phase 1 of the Support Study).

Specifically, the architecture of the EU PKI ecosystem for e-mobility is composed by three main components:

- the European Commission's PKI **governance elements**;
- the **PKI system(s)** onboarded in the ecosystem;
- the **Certificate Pools** and services.

The image below outlines the EU PKI ecosystem for e-mobility

Figure 13: Graphic representation of the EU PKI ecosystem

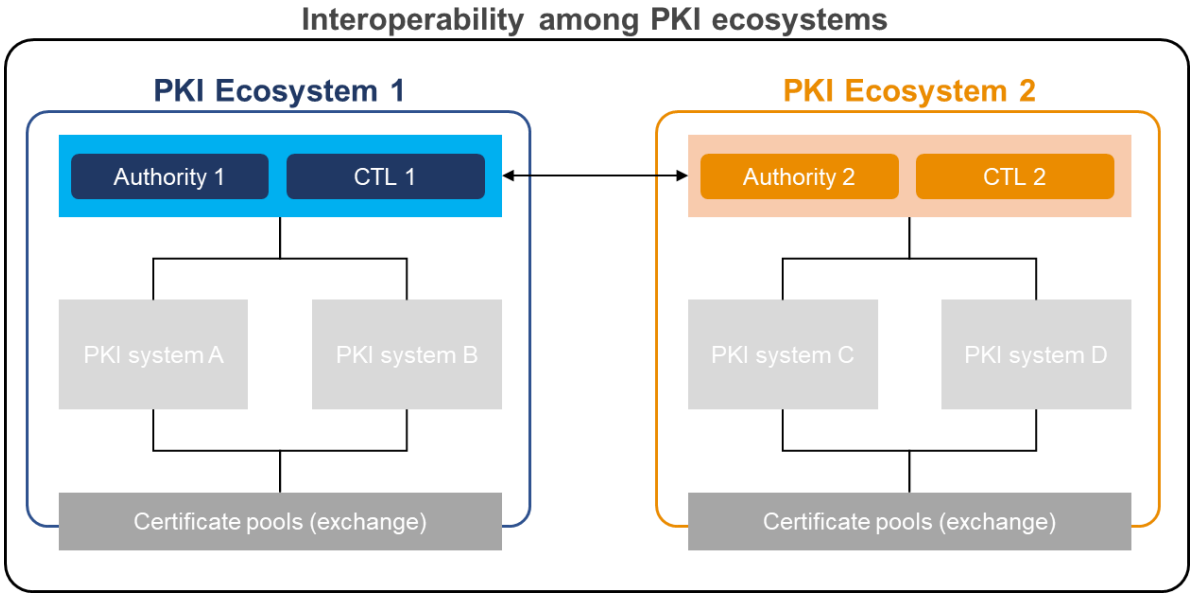


To achieve a fully functional governance of the PKI ecosystem, the establishment by the European Commission of the following governance bodies is envisaged:

- The **e-mobility PKI ecosystem Governance body (ePEGMB)** covers the top sub-role of the overall governance architecture. The role of the body is to **set rules and requirements** for the whole EU PKI ecosystem, as well as to **establish and maintain the policies** that regulate the ecosystem over time;
- The **e-mobility PKI ecosystem Operating Body** (ePEOB) is responsible for running the elements required to achieve interoperability within the PKI ecosystem, with its PKI systems, through the CTL approach. Procedurally, the Operating Body would be composed by the following components:
    - **Trust List Manager** (TLM): it represents the unique centralised role that **holds the "TLM Certificate"** used to sign the CTL. The TLM Certificate is the **highest cryptographic certificate trust anchor**. The TLM is responsible for the update of the CTL on the basis of the inputs of the so-called e-mobility Point of Contact (ePOC), by including the newly accepted Root certificates as well as for the removal of the expired and revoked ones;
    - **e-mobility Point of Contact** (ePOC): it **collects applications** from all operational Root CA certificates in the EU. Moreover, it **publishes the CTL** created by the TLM. It has therefore an **external coordination role**, acting as an entry point for companies that want to apply for and or consult the CTL. It accepts or rejects the application of PKI Root operators to be included in the CTL and distributes the CTL;
    - **Operations Manager**: it has an **internal coordination role** (opposed to the external coordination role of the ePOC). Its main function includes the **implementation of the operational requirements** published by the Operation Governing Body, operating specific e-mobility infrastructure, and escalating **incident reports** to the Operation Governance Body. Specifically, it **coordinates the operation of the system** and interfaces with the stakeholders. It is the actor responsible for the organization of CTL signing sessions.

In the case of **multiple PKI ecosystems** for e-mobility being established, reaching **interoperability at ecosystem level** should be explored. This could be achieved through a **coordination effort among the governance authorities of the different PKI ecosystems**. This would aid in lifting the burden from the PKI systems - already onboarded in the CTL of one of the PKI ecosystems – of having to enrol in another additional PKI ecosystem. However, the specific solution to enable interoperability between the CTL of different PKI Ecosystems would need to be developed cooperatively as soon as the need arises. The image below exemplifies a potential interoperability scheme at ecosystem level between two PKI ecosystems. The same approach would still be valid with a greater number of ecosystems.

Figure 14: Interoperability among PKI ecosystems



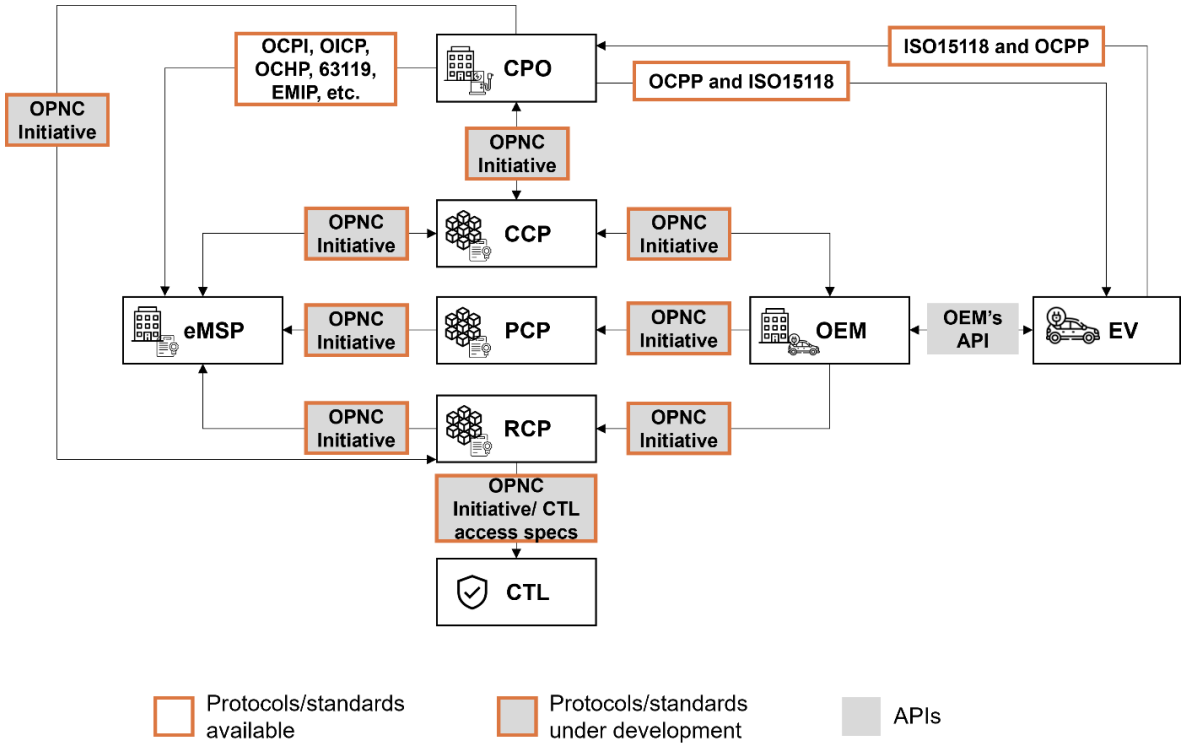
Deliverable 2 - Relevant standards and technical aspects of the PKI to allow interoperability across Root CAs

The objective of the second deliverable is to **identify the standards and technical aspects of the PKI** (e.g., APIs) enabling **interoperability across Root CAs** and the different participants to the Plug&Charge (e.g., CPOs, EMSPs, EVs, EVSEs, etc.).

The document starts from an **analysis of the standards and technical specifications currently available** in the market. Then, it proceeds to capture what is still **under development** (i.e., OPNC initiative) or **missing** and it proposes an action plan to **fill the existing gaps**. Subsequently, it is outlined the **communication flow** required to enable Plug&Charge in association with the standards and protocols required to enable it (see Figure 15). The document includes a detailed table on this matter.

The figure below illustrates the standards and APIs available or under development to enable P&C based on ISO 15118 and the preferred governance and architecture reflected in this Support Study.

Figure 15: Overview of protocols, standards and APIs enabling Plug&Charge



Based on the analysis, in terms of the **actions to take** to tackle the standards and technical aspects missing or still under development, first of all the European Commission will mandate the European Telecommunications Standards Institute (ETSI) for the **development of the relevant specifications for the CTL its accessibility** to all participants to the EU PKI ecosystem for e-mobility. This specification will enable the ecosystem interoperability by allowing all ecosystem participant to **directly access the content of the CTL**.

Additionally, the CTL could be accessed by the ecosystem participants (i.e., eMSPs, OEMs, CPOs, EVs) **indirectly**. This could be done through the use of the **Certificate Pools**. The latter would directly access the CTL through the aforementioned specifications and redistribute its content to the other participants.

In this regard the **OPNC Initiative** within CharIN is expected to play a fundamental role as it aims at developing a **protocol** which will cover the **communication from PnC actors** (i.e., OEMs, CPOs, and EMSPs, etc) **to the Certificate Pools** and vice versa.

As the OPNC Initiative's protocol is still under development the European Commission agreed with CharIN on two important aspects:

- to **collaborate on the OPNC initiative development** and include relevant topic for discussion in the STF;
- once the OPNC Initiative's protocol is ready, to **submit it to a standardisation organisation** such as IEC/ISO. The ultimately goal is to give raise to an international standard with global market acceptance.

Deliverable 3 - Market rules for the EU PKI ecosystem for e-mobility

In the third deliverable developed within the Support Study, the **market rules for the EU PKI ecosystem for e-mobility are outlined**.

The first section of the document focuses on the market rules and includes a full set of guidelines for:

- the **bodies and actors falling under the European Commission governance** (under Deliverable 1 – Architecture, governance, and operating models for a PKI based on ISO 15118);
- **onboarding** (and offboarding) in the PKI Ecosystem and in the PKI Systems;
- **PKI Systems**;
- Pools and services;
- **Participants** of the EU PKI ecosystem for e-mobility (i.e., CPOs, EV-OEMs, EMSPs, etc.).

This section of the document has been fully developed with the working group and validated by the STF Sub-group on G&S, the European Commission and the JRC.

Conversely, the second part of this document was also initially expected to reflect the **onboarding guidelines.** At the moment of finalising this Support Study, these guidelines are in a draft form (at disposal of the European Commission and participant members of the working group). Upon accordance with the European Commission, the revision and fine-tuning process of these guidelines was **suspended to prioritise other deliverables** of the Support Study. Consequently, PwC advises that the onboarding guidelines undergo a final process of revision and further development by a group of experts selected by the European Commission.

Deliverable 4 - Mutually recognised set of criteria for Root CAs, Subscribers and the CTL of the EU PKI ecosystem for e-mobility

The objective of the fourth deliverable is to delineate a set of **mutually recognised criteria for some of the key participants of the EU PKI ecosystem for e-mobility**. Specifically, in the document are laid out the requirements to be a **trustworthy Root CA operator** within the EU PKI ecosystem for e-mobility, for **subscribers** to the PKI, and lastly a set of **general requirements for the CTL** of the EU PKI ecosystem for e-mobility.

Originally this deliverable also was expected to include a series of **minimum requirements** applicable to **Certificate Policy** (CP) documents within the EU PKI ecosystem for e-mobility. At the moment of finalising this Support Study, these minimum requirements are in a draft form (at disposal of the European Commission and participant members of the working group). Upon accordance with the European Commission, the **development of the minimum requirements for the CP were suspended to prioritise other deliverables** of the Support Study. Consequently, PwC advises to finalise the development of the minimum requirements for the CP and to undergo a final process of revision and further development by a group of experts selected by the European Commission.

Deliverable 5 - Implementation plan for the preferred governance and architecture model

In the context of this Support Study, the fifth deliverable aims at reflecting the **proposed way forward by the European Commission** in order to support the development of an EU PKI

ecosystem for e-mobility. The document was drafted by PwC, the European Commission, and the JRC considering all the discussions occurred during the Support Study development and only afterwards validated through the working group and the STF Sub-group on G&S.

In concrete terms, this deliverable describes the **concrete actions** needed in order to **set-up and implement the high-level governance and architecture framework** elaborated in this study and considering the recommendations by the STF Sub-group on Governance and Standards (Activity 2). In that regard, this document gathers the concrete steps in terms of **legislative process** (AFIR delegated/implementing acts), **governance bodies set-up** and PKI **technical implementation** and operation to put in place an EU PKI ecosystem for e-mobility based on a regulated framework to a Multi-Root CA model with the CTL as the interoperability solution. For a complete understanding of the **implementation roadmap**, this deliverable should be read alongside Deliverable 1 on the "Development of a governance, architecture, and operating model for a PKI based on ISO 15118".

Finally, it is important to note that this deliverable presents a **proposed approach** that the European Commission could follow to reach the **preferred governance and architecture defined in Deliverable 1**. However, it is ultimately a decision from the European Commission to endorse and carry out the roadmap elaborated in this deliverable.

4 Support Study's main achievements

The Support Study main achievements are summarised in the following points:

- The **generation of consensus** in a wide and diverse group of stakeholders starting from diverging views on the PKI governance and architecture for the EU, including the concrete use case of Plug & Charge;
- **Definition of the main features of a future EU PKI ecosystem for e-mobility** in relation to ISO 15118;
- Development of an agreed upon **set of definitions for the EU PKI ecosystem for e-mobility;**
- **Definition of a proposed governance and architecture** framework for the potential future EU PKI ecosystem for e-mobility;
- Definition of a **clear way forward to fill the standardization gaps of an interoperable architecture based on the CTL**, including:
    - New **European Commission standardisation request** to ETSI to cover the EU PKI CTL requirements;
    - **Agreement to work with EU industry through the OPNC taskforce** within CharIN to address other relevant standardisation aspects;
    - **Upcoming coordination with STF Sub-group on Governance & Standards for further endorsement and submission of OPNC** to international standardization organization (IEC or ISO).
- **Draft of a new full set of market guidelines for the EU PKI ecosystem**, its participants (PKI Systems, PKI operators, Root CAs, OEMs, CPOs, EMSPs, Certificate Pools and Services), and the EU Governance components (ePEGMB, CTL, TLM, ePOC, EPEOB), considering input by relevant stakeholders;

- **Definition of the structure of the implementing act** under AFIR for the establishment and operation of the EU PKI ecosystem for e-mobility and the draft contents of the related annexes;
- Overall development of an innovative work, based on an open public and private dialogue and cooperation, that could serve also as a **reference for other regions** for the creation of **open and freely competing e-mobility markets** based on common rules and definitions.

5 Follow-up to the Support Study

The establishment and operation of the EU PKI ecosystem for e-mobility will require a series of regulatory (policy) steps as well as a number of key technical actions. The most critical steps and key actions to reach the full implementation of the EU PKI ecosystem for e-mobility are reflected on the list below:

- **Decision by the European Commission** on the proposed approach to the **governance and architecture** interoperability of the EU PKI ecosystem for e-mobility (Q4 2023).
- Adoption by the European Commission of the **relevant delegated and implementing acts** in support of the EU PKI ecosystem for e-mobility (Q4 2023 – Q3 2024).
- **Set-up** by the European Commission **of the relevant bodies** (expert groups) for the management and operation of the EU PKI ecosystem (Q2 2024).
- Development by European/International Standardisation Organisations and market actors of the **CTL technical specifications** and **relevant protocols** for the functioning of the EU PKI ecosystem (Q1 2025).
- Start of the technical work on the EU PKI CTL interoperability by EC or delegate such as JRC (Q1 2025).
- Full implementation (Q1 2026).

In view of the aforementioned steps required for the establishment and operation of the EU PKI ecosystem for e-mobility, the Support Study allowed a **considerable acceleration** in the production of content on the topics addressed in the five deliverables captured in this final report.

Considering the limited timeframe and the complexity of the technical discussions, it was not possible to conclude the full content initially foreseen for the technical deliverables as part of the Support Study. PwC together with the European Commission agreed on **prioritising the development of those deliverables which would set the foundation of the EU PKI ecosystem for e-mobility and the preparation of upcoming implementing act**. Consequently, together with the aforementioned milestones it is of paramount importance to **finalise the deliverables** which, for the sake of prioritisation, were **left incomplete (draft stage)**. Specifically, in order to promote the smooth functioning of the EU PKI for e-mobility it would be **required to finalise and validate with industry experts the following content**:

- **Security Policy (SP)** for the deployment and operation of the EU PKI ecosystem for e-mobility;
    - Starting from the SP of the reference practice C-ITS, PwC has prepared a draft of the SP for the EU PKI ecosystem for e-mobility. The SP is an essential element for the smooth and secure operation of the PKI. PwC suggests to the

European Commission to finalise this document and include relevant aspects in the implementing act for the EU PKI ecosystem.

- **Certificate Policy (CP)** for the EU PKI ecosystem for e-mobility.
    - Starting from the CP of other PKI service providers and considering the reference practice C-ITS, PwC has prepared a draft of the CP for the EU PKI ecosystem for e-mobility. The CP is a key element that underpins the policies, procedures and technical details related to the issuance and control of certificates in the EU PKI ecosystem. PwC suggests to the European Commission to finalise this document and include relevant minimum requirements in the implementing act for the EU PKI ecosystem for e-mobility applicable to all CPs of PKI service providers.

- **Onboarding Guidelines** for the EU PKI ecosystem for e-mobility
    - Starting from the onboarding guidelines of other PKI service providers and considering the reference practice C-ITS, PwC has prepared a draft of the onboarding guidelines for the EU PKI ecosystem for e-mobility. The onboarding guidelines are essential to ensure the inclusion and participation of market actors. PwC suggests to the European Commission to finalise this document and include relevant aspects concerning onboarding guidelines in the implementing act for the EU PKI ecosystem for e-mobility.

Relevant documentation and bibliography

For the elaboration of this document and its annexes the following documentation was considered.

- CharIN (2020). CP for ISO 15118 V2G PKI. Available here.
- CharIN (2022). Certificate Policy for the CharIN V2G first-generation PKI (compliant to ISO 15118-2). Available here.
- CharIN (2022). Plug and Charge Europe Terms & Conditions of Charging Interface Initiative e.V. Available here.
- CharIN (2023). Whitepaper of Charging Interface Initiative e.V. Available here.
- ElaadNL (2018). Exploring the Public Key Infrastructure for ISO 15118 in The EV Charging Ecosystem. Available here.:
- ElaadNL (2022). Public Key Infrastructure for ISO 15118 Freedom of choice for consumers & an open access market. Available here.
- European Commission (2017). Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS). Available at: https://transport.ec.europa.eu/system/files/2018-06/c-its_security_policy_release_1.pdf
- Euroean Commission (2019). COMMISSION DELEGATED REGULATION (EU) …/... of 13.3.2019 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems. Available here.
- European Commission (2018). Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS). Available here.
- Hubject (2020). Certificate Policy – ISO15118 V2G PKI Hubject Plug&Charge. Available here.
- IEA (2022). Grid Integration of Electric Vehicles - A manual for policy makers. Available here.
- STF Sub-group on Governance & Standards (2022). Activity 1, Mapping of the discussion concerning standards and protocols for communication exchange in the electromobility ecosystem. Available here.
- STF Sub-group on Governance & Standards (2023). Activity 2 – Block 3 report working group report on regulatory needs and other outstanding technical aspects. Available here.

Annex – Deliverables of the Support Study (Phase 2)

The following finalised deliverables, corresponding to Phase 2 of the Support Study, are attached as an Annex to this final report.

- **Deliverable 1** - Architecture, governance, and operating models for a PKI based on ISO 15118
- **Deliverable 2** - Relevant standards and technical aspects of the PKI to allow interoperability across V2G Root CAs
- **Deliverable 3** - Market rules for the EU PKI ecosystem for e-mobility
- **Deliverable 4** - Mutually recognised set of criteria for Root CAs, Subscribers and the CTL of the EU PKI ecosystem for e-mobility
- **Deliverable 5** - Implementation plan for the preferred governance and architecture model

ANNEX
SUPPORT STUDY PHASE 2 DELIVERABLES

This annex contains the completed deliverables of Phase 2 of the Support Study.

TABLE OF CONTENTS

EUROPEAN COMMISSION
Directorate-General for Mobility and Transport

Directorate B – Investment, Innovative & Sustainable Transport
B4 – Sustainable & Intelligent Transport

EUROPEAN COMMISSION SUPPORT STUDY

DEVELOPMENT OF A GOVERNANCE FRAMEWORK FOR THE EU PUBLIC KEY INFRASTRUCTURE (PKI) BASED ON THE STANDARD ISO 15118

DELIVERABLE 1 - ARCHITECTURE, GOVERNANCE, AND OPERATING MODEL FOR A PKI BASED ON ISO 15118

Objective: The aim of this deliverable is to define the **governance, architecture, and operating model** for a EU PKI based on ISO 15118, in line with recommendation of Phase 1 of the Support Study.

The activity will build on the work carried out by the members of the working group set up and coordinated under the European Commission Support Study.

Extension: To be discussed.

Foreword

This document is a deliverable in support of the preparation of secondary legislation (i.e. delegated and/or implementing acts) under the Alternative Fuels Infrastructure Regulation (AFIR)[22]. This concrete deliverable elaborates on the development of a governance, architecture, and implementation plan for the set-up and operation of an EU Public Key Infrastructure (PKI) ecosystem in the EU.

The document has been developed as part of the European Commission 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC. The document has also been reviewed and validated by the Sustainable Transport Forum (STF), which is established and chaired by the European Commission services since April 2015 to assist the Commission in implementing the Union's activities and programmes aimed at fostering the deployment of alternative fuels infrastructure to contribute to the European Union energy and climate goals.

The study was articulated in two phases.

Phase 1 of the 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC.

During the first phase, the study was centred around bilateral interviews with the existing PKI service providers and research projects of the Sustainable Transport Forum (STF) subgroup on Governance & Standards - namely CharIN, Gireve, Hubject, SAE, and Vedecom. The result of this phase has been the development of a set of recommendations on a high-level governance and architecture framework for the functioning and operation of a PKI ecosystem in the EU. These recommendations were later transmitted and reviewed by the STF sub-group on governance and standards, being those endorsed by the sub-group as part of the document *Activity 2 - 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*[23].

- **Recommendation 1: A regulated vs. non-regulated governance and architecture –** the STF sub-group favours a regulated approach for the governance and architecture in Europe due to the advantage of providing a clear legal basis covering key elements of the PKI.
- **Recommendation 2: Single or Multi Root CA model** - The STF sub-group members advocate for a multi-Root CA model due to the benefits of having competition in the market among several V2G Root CAs – increased variety and quality of service, reduced prices - as well as the increased operational resilience of the PKI. Also, this approach also supports the current market situation under which multiple market actors are already committed to offering the service of V2G Root CA in the EU.
- **Recommendation 3: Architecture model to ensure interoperability across Multi Root CAs** - the STF sub-group members' preferred interoperability solution across the

[22] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1867

[23] https://op.europa.eu/en/publication-detail/-/publication/b7910659-276c-11ee-839d-01aa75ed71a1/language-en

multi-Root CA model is a Certificate Trust List (CTL), due to the solution's potential for scalability, centralised maintenance, and fitting logic of certificate verification.

- **Recommendation 4: Governance Model –** the STF sub-group members on G&S prefer a mixed approach, involving both private and public stakeholders. The combination of categories of entities such as businesses organisation, industry consortia and public authorities allows to leverage the strengths of each of them while minimising the downsides.
- **Recommendation 5: Ownership model** – the STF sub-group members on G&S agree on having a central public authority (i.e. European Commission) to perform the governance roles of the PKI (i.e. Definition of criteria for Root CAs operators, check of the criteria, and distribution of the CTL) while the managing and operating layer of the multiple PKI systems (i.e. operations of the PKI and the actual provision of the emission of certificates and signing service) could be covered by a combination of business organisations, industry consortia and public authorities.
- **Recommendation 6: Implementation scheme for the proposed governance and architecture solution** – the STF sub-group members on G&S agree that the development of the preferred governance and architecture solution will most likely occur in two phases. The initial phase will see the continuing of the existing Plug & Charge service solutions with their corresponding PKI implementations where the market is further tested and scaled-up by market actors. This relates in particular to existing implementations of ISO 15118-2. The second phase will be based on a regulated approach by the European Commission under a set of governance and architecture rules applicable in the EU considering the elements developed in the deliverables of this study and the recommendations of the STF Sub-group. A future PKI ecosystem will consider existing implementations based on ISO 15118-2 and, at the same time, will transition towards a future based on ISO 15118-20.

Phase 2 of the 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC.

The second phase of the study builds on the recommendations of the previous phase. Specifically, a dedicated group of experts was specifically formed to work on the following set of deliverables aiming to define the policy, technical and governance elements to guide the set-up and develop a regulated approach to a Multi-Root CA model with the CTL as the preferred interoperability solution. All this, under a mixed (public/private) governance approach:

Table 14: List of deliverables completed under the Support Study

Deliverable	Title
1	**Deliverable 1** - Architecture, governance, and operating model for a PKI based on ISO 15118;
2	**Deliverable 2** - Relevant standards and technical aspects of the PKI to allow interoperability across V2G Root CAs;
3	**Deliverable 3** - Market rules for the EU PKI ecosystem for e-mobility;

4	**Deliverable 4** - Mutually recognised set of criteria for Root CAs, Subscribers and the CTL of the EU PKI ecosystem for e-mobility;
5	**Deliverable 5** - Implementation plan for the preferred governance and architecture model;

More specifically, the present deliverable is the result of the work of the working group coordinated under the European Commission 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC. The organisations comprising the working group are the following members of the STF subgroup on Governance & Standards:

- CharIN,
- Gireve,
- Hubject,
- SAE,
- Vedecom,
- ChargePoint,
- ElaadNL,
- EnBW,
- Shell,
- Smartlab,
- Tesla,
- E-clearing.net.

The work developed by the working group and reflected in these deliverables has been also subject to the review and validation of the Sustainable Transport Forum (STF) Sub-group on Governance & Standards.

Scope of Deliverable 1

In the context of the Support study, Deliverable 1 is of utmost importance for the whole **conceptualization of the governance and architecture framework of the EU PKI ecosystem**. This document outlines the concrete governance and architecture requirements as well as the roles and responsibilities of the different bodies within EU PKI ecosystem, thus, establishing the interface between the EU PKI ecosystem and the multiple potential PKI systems.

First, **this deliverable gathers the main definitions applicable to the entire support study** and, subsequently, to all the relevant documents and materials produced (e.g., certificate and security policies, market rules, technical specifications, etc.). Here, the **clear differentiation between EU PKI ecosystem and PKI system is critical** for a sound understanding of the whole governance and architecture approach in the EU.

The **harmonisation of definitions by industry actors in alignment together with the EU legislator is essential** to develop a common understanding that allows to put in place a regulated approach that effectively supports market actors and facilitates the development of a level playing field backed-up by EU legislation. Without this critical step, it would have not been

possible to develop a first use case applied to Plug & Charge, but neither to potentially endorse other use cases that might arise in the future.

Second, this deliverable elaborates the main governance bodies and architecture elements for the set-up and operation of a EU PKI ecosystem according to the high-level criteria previously defined both in Phase 1 of the Support study and, mor generally, in Activity 2 - *Development of a governance and architecture framework for the implementation and operation of a Public Key Infrastructure (PKI) ecosystem in the EU*.

Finally, it is important to mention that the term PKI ecosystem for e-mobility in the context of PKI governance, architecture, and operating model in this document relates to the Plug and Charge (PnC) use case. However, **the governance and architecture approach has been designed in a manner that would be fully applicable to other future use cases**, thus, it is not limited solely to the Plug & Charge use case, albeit currently is the main one. As a consequence, the EU PKI ecosystem for e-mobility and its governance, architecture, and operating model will be capable of endorsing other use cases including those that might arise in the future.

1 Introduction

In the deliverables developed during Phase 2 of the *Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118* the definitions described in this chapter are adopted. The use of commonly agreed definitions it is of critical importance to ensure technical coherence and homogenous level of interpretability among the different deliverables and documents reflecting the governance, architecture and operation of the PKI ecosystem in the EU.

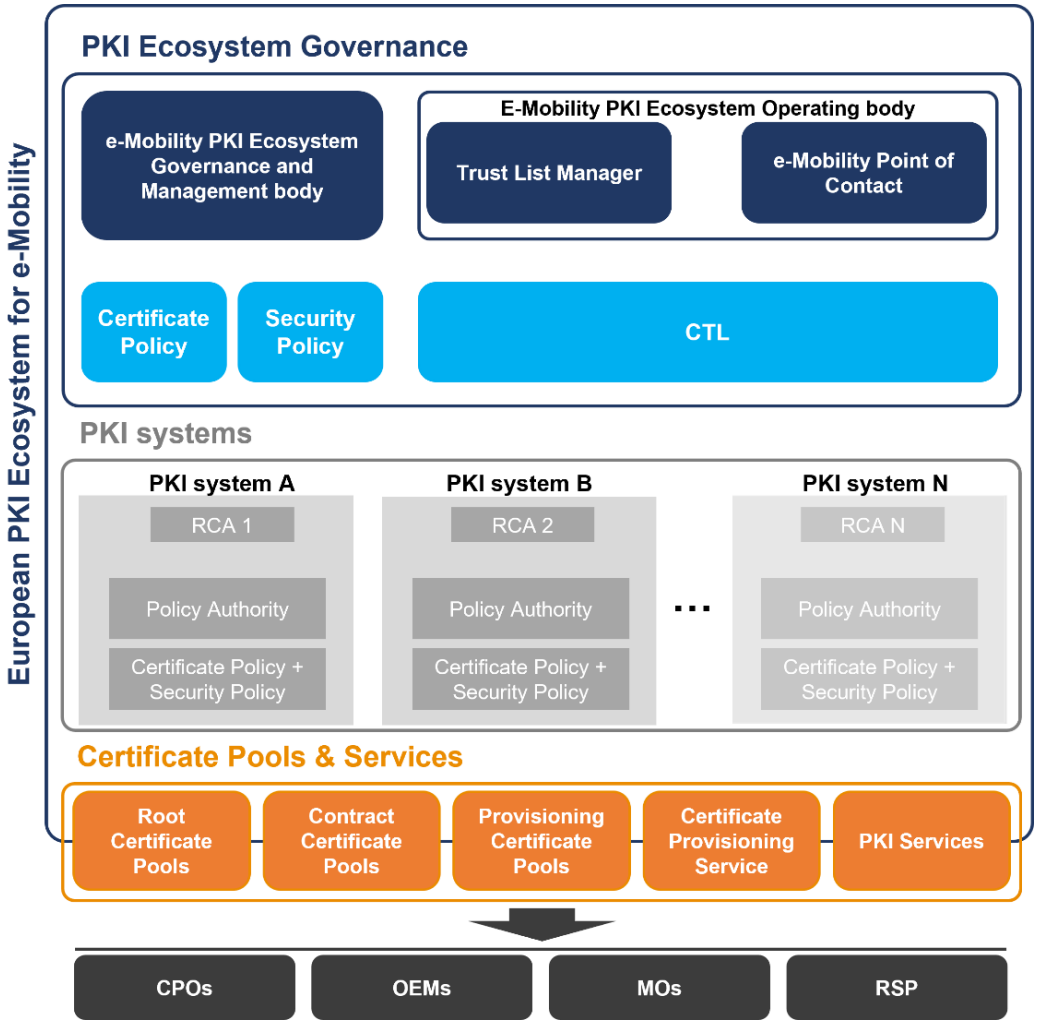
2 EU PKI ecosystem for e-mobility

In the context of e-mobility, a ***PKI ecosystem*** is 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). This 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 via the CTL approach thus with the purpose of achieving interoperability inside the PKI ecosystem. The e-Mobility PKI ecosystem Governance and Management body, therefore, will be responsible for on-boarding, this includes checking that the auditing requirements of the PKI system RCAs are fulfilled, and the audits have been carried out by accredited independent PKI auditors.

A 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”.

The image below offers a visual representation of the definition of PKI ecosystem through the example under development in this study of a European Union PKI ecosystem for e-mobility. In the particular case of other PKI ecosystems outside the EU, the central authority role it is expected to be held by the relevant organization determined in such ecosystem.

Figure 16: Graphic representation of the EU PKI ecosystem



* For other PKI ecosystem, the central authority would be determined by such ecosystem.

Albeit interoperability among different ecosystems is out of scope for this deliverable, **if multiple PKI ecosystems are to coexist globally, it would be possible to reach interoperability among them (at ecosystem level) if all the elements to ensure reciprocal trust are reached** (i.e., ecosystem rules, Certificate and Security Policy requirements, market rules, etc.). With this approach, instead of leaving the burden and associated operational risks for PKI systems to find connections with one another, the central authorities of the multiple PKI ecosystem might recognize one another trustworthiness thus reflecting it upon all the individual PKI system composing them.

In the EU PKI ecosystem context, the European Commission as central authority, with its corresponding governing body, would be responsible for discussing and establishing interoperability with other PKI ecosystems. **PKI systems from other PKI ecosystems to be accepted in the EU ecosystem would have, therefore, to endorse a series of elements (i.e., ecosystem market rules, Certificate and Security Policy requirements, etc.) that would ensure a level playing field in line with the EU governance and architecture principles**. Looking further, the concrete interoperability between different ecosystems would need to be addressed by the e-mobility PKI Ecosystem Governance and Management body.

3 PKI system

A PKI system is a secured environment centred around a single Root Certificate Authority (Root CA) that a PKI participant (entity CPO, EV-OEM or EMSP) can use to enable secure authentication and authorisation via Plug & Charge in accordance with ISO 15118. Additionally, a PKI system has its own Policy Authority in charge of publishing and updating its Certificate and Security Policies. If several PKI participants can use the same Root CA jointly, it would be considered a "***shared PKI system***". In this case, the Root CA is managed by a PKI provider that operates the PKI system and may offer additional services (i.e., Pool management services). Conversely, a "***dedicated PKI system***" is used by and for a single PKI participant and centred around a Root CA operated by the same participant. Both shared, and dedicated PKI systems are recognised as part of the EU PKI CTL system architecture and comply with the EU PKI ecosystem governance rules.

4 Other definitions

Certificate: 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): It means a set of rules that indicate 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): It 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[24]. [ISO/IEC 27099:2022]

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

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): It is a list of all trusted Root Certification Authorities 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 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.

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): It is a bundle of data containing mainly the Contract Certificate used to ensure integrity and authenticity. The CB when signed by the CPS is called “Sign-Certificate-Bundle”.

Contract Owner (CO): It is the person in possession of a valid “Plug & Charge” EMSPEMSP 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.

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 Plug & Charge service after activation. The EV driver is able to: 1) activate or deactivate P&C and 2) manage P&C contract preferences by means of vehicle User Interface (i.e. app or in-vehicle display).

E-mobility Service Provider (EMSP)[25]: 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.

Provisioning Certificate Identifier (PCID): It identifies the OEM Provisioning Certificate. Will be used to connect an EV to a contract in the contract certificate that will be used to support the PnC feature.

PKI participant: Entities which make use of a PKI system, i.e. CPO, EV-OEM or EMSP. The entities 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. The EMSPscan 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.

[25] 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. For the purpose of this study the term V2G will be used to refer to communication between EV and EVSE.

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)

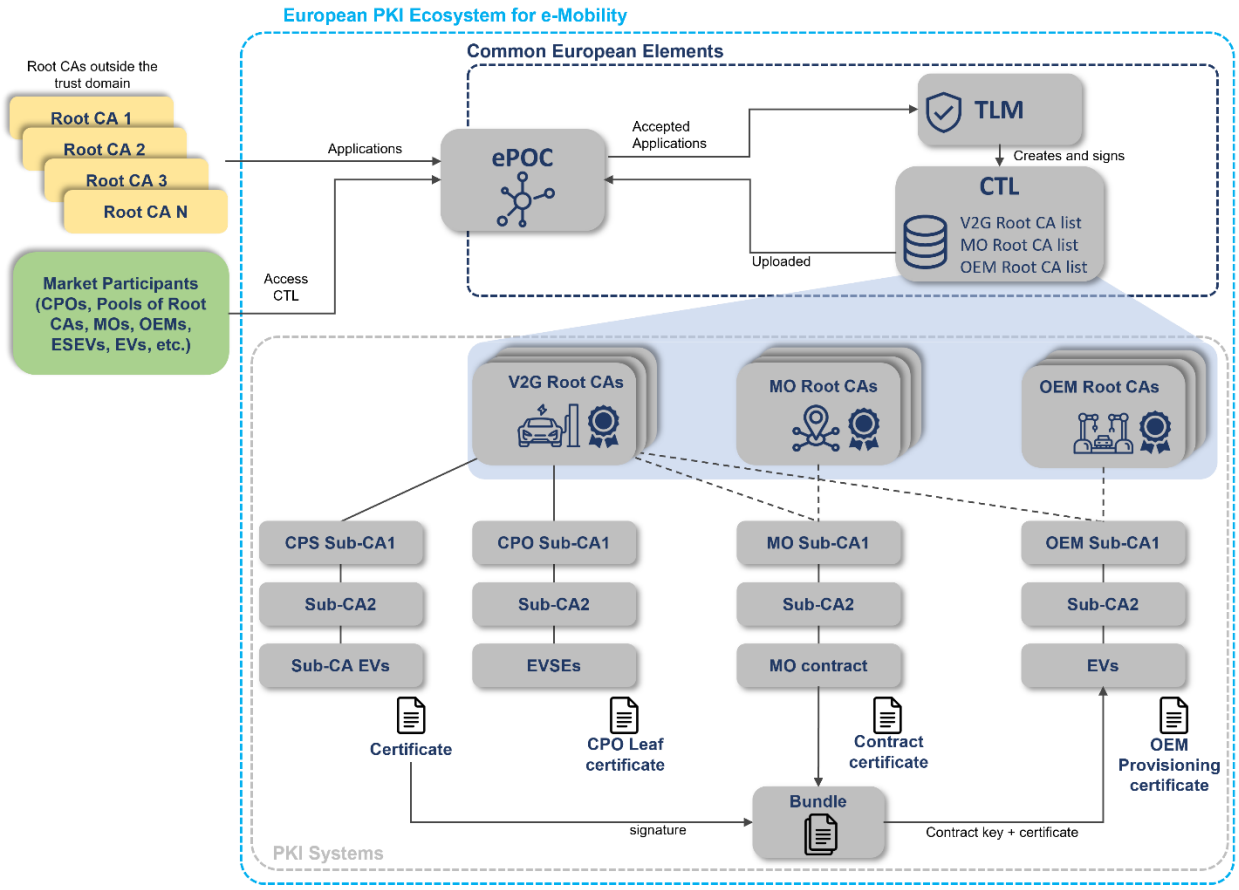
Vehicle2Home (V2H): It means the control of time, magnitude and direction of (dis)charging power from a home power source to the EV and back to a home power source.

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.

5 Architecture for a EU PKI ecosystem for e-mobility

As emerged from the first phase of the support study, the recommended architecture for interoperability of the EU PKI ecosystem for e-mobility is the CTL approach integrating multiple potential PKI systems based on ISO 15118 (both with current version -2 and incorporating -20 in the future, until a full transition towards -20 occurs). It 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. In the EU, the role of the TLM would be covered by the European Commission (or a delegate). The European Commission would ensure neutrality and the joint and equal representation of the interests of the different actors in the market.

Figure 17: Architecture model for the EU PKI ecosystem for e-mobility



The model above provides a graphic representation of the elaborated architecture model for the EU PKI ecosystem for e-mobility based on the standard ISO 15118. The architecture model is divided in the following two areas:

1) The **Common European Elements** (enclosed in the blue dotted line) contains the roles and actors enabling the setup of interconnections in a secure and interoperable manner through the Certificate Trust List (CTL) approach. The Common European Element area serves the function of establishing and maintaining a trust environment for the European e-mobility PKI ecosystem. Specifically, it mediates the relationship with the market PKI systems by regulating the access of external Root CAs (in yellow) in the trust

environment through the application of the CTL approach to governance and the inclusion of a centralised communication channel named e-Mobility Point of Contact (ePOC). The detailed description of the Common European Elements (ePOC, CTL, TLM) as well as their role will be covered and elaborated in the next chapter.

2) The **PKI systems** (enclosed in the grey dotted line) whose Root CA is included in the CTL (enclosed in the light blue area) are part of the European PKI ecosystem for e-Mobility. Figure 3 provides a graphic representation of the flow of certificates from the Root CAs down to the end-entities (EVs and EVSEs). All technical aspects on this matter are elaborated in the text of the standard ISO 15118[26], thus, this document it focuses on the overall architecture ecosystem and operational aspects of the governance approach.

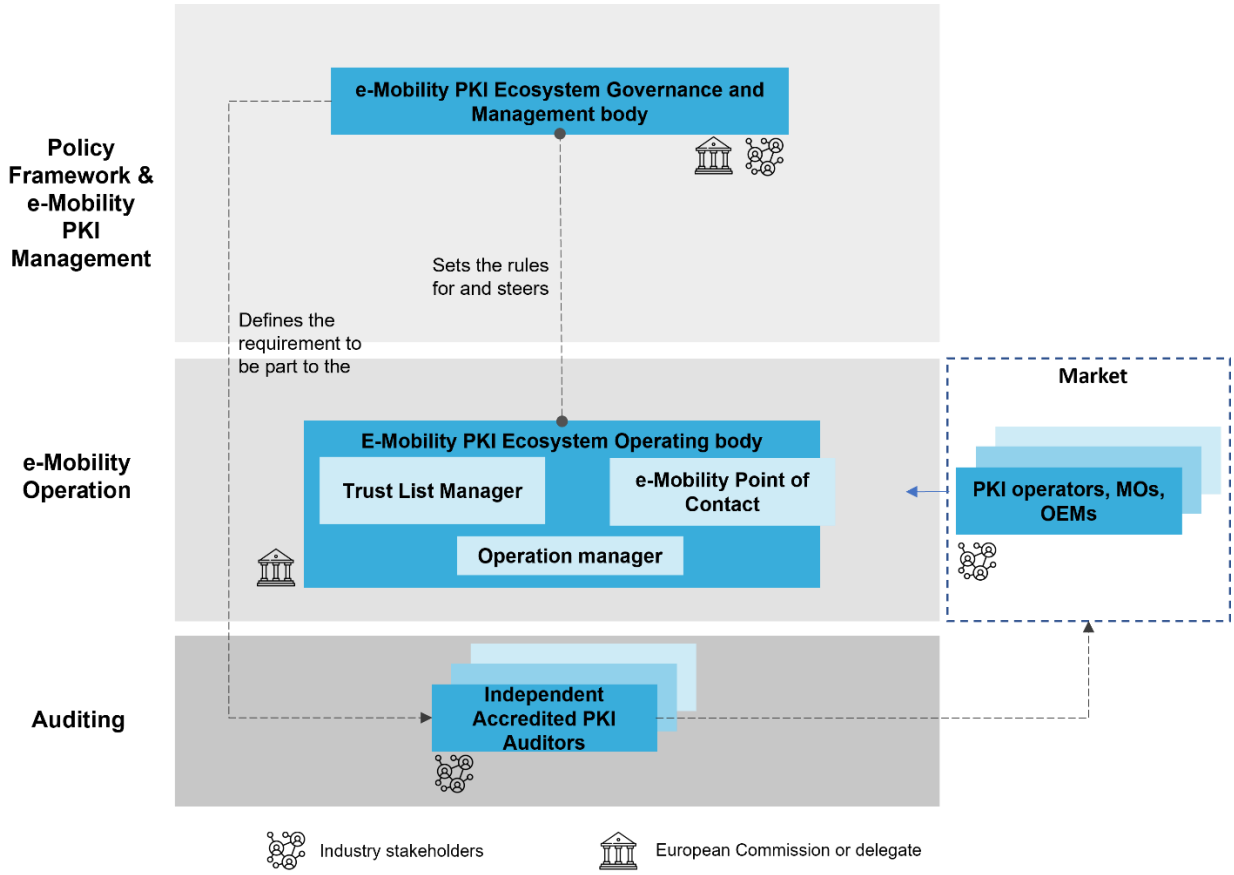
6 Governance model for a EU PKI ecosystem for e-mobility

As per recommendations 4 and 5 of the first phase of the support study, the recommended governance of the EU PKI ecosystem is a “mixed approach” option, where one public authority (i.e., the European Commission or a delegate) 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, including the offering of Plug & Charge services.

[26] **ISO 15118-2:2014** Road vehicles — Vehicle-to-Grid Communication Interface — Part 2: Network and application protocol requirements. Available at: https://www.iso.org/standard/55366.html

ISO 15118-20:2022 Road vehicles — Vehicle to grid communication interface — Part 20: 2nd generation network layer and application layer requirements. Available at: https://www.iso.org/standard/77845.html

Figure 18: Governance model for the EU PKI ecosystem for e-mobility



The image above represents the governance model for the e-Mobility EU PKI based on ISO 15118. This governance model is structured based on the feedback collected from previous consultations of the Support study (Phase 1), recommendation 3 of Activity 2 Block 2 and, importantly, the governance model of the EU C-ITS PKI that has been used as a reference.

The governance model is divided into three levels:

1) **Policy framework & e-Mobility PKI management**: it concerns the creation and update of policies (Certificate and Security Policies) and rules for the e-Mobility PKI ecosystem as well as their enforcement and compliance control;
2) **e-Mobility PKI operation**: it concerns with the actual operation of the e-Mobility PKI's governance and interoperability through the CTL approach.
3) **Auditing**: it concerns the compliance checking of Root CA, CTL, Trust List Manager (TLM) and ePOC on the basis of the requirements set by the ePEGMB.

The different levels of the governance model require a series of governance bodies in order to provide guidance, steer and operate the EU PKI ecosystem for e-mobility. The roles and responsibilities of these bodies (captured in Figure 4) are detailed in the following sub-sections.

6.1 E-mobility PKI Ecosystem Governance and Management body

The e-Mobility PKI Ecosystem Governance and Management body (ePEGMB) covers the top sub-role of the overall governance architecture and operates at the policy framework level. In the case of an EU PKI ecosystem for e-mobility, it should be composed by a group of experts from the European Commission, Member States, and a homogeneous representation of stakeholders from the industry with interest in the offering of Plug & Charge services in the EU (i.e., PKI project providers, equipment manufacturers, vehicle manufacturers, etc.). The participation in the group is to be defined typically through the launch of a call for applications by the European Commission. The group will count with its corresponding Terms of Reference (ToR) and Rules of Procedure (RoP).

The role of the group is to set rules and requirements for the whole EU PKI ecosystem, as well as to establish and maintain the policies that regulate the ecosystem over time. As a matter of fact, in terms of governance, the ePEGMB is responsible for:

- Establishing a general strategy applicable to the EU PKI ecosystem in line with potential regulatory aspects established in the EU for the management and operation of an EU PKI ecosystem.
- Dealing with technical aspects of the deployment and operation of the e-Mobility PKI system.
- Approving the Certificate and Security Policies as well as their future changes requests and decision of the release of new policy versions.
- Overseeing the e-Mobility PKI compliance assessment operations and the definition of the governing rules and procedures for the compliance assessment tests and procedures.

This body will also be in charge of discussing, negotiating and potentially establishing connection and recognizing PKI systems, with their Roots CAs, included in other e-Mobility PKI ecosystems (e.g., a future US PKI ecosystem).

In terms of management, it is responsible to compile and maintain the operational requirements based on:

- The strategy from the e-Mobility PKI Ecosystem Governance Body
- The Compliance Assessment Reference Framework
- The Certificate and Security Policies

The management role is to set up and coordinate the systems in place to ensure the proper functioning of the EU PKI ecosystem on the basis of what is established by the e-Mobility PKI Ecosystem Governance model.

As anticipated above, the e-Mobility PKI ecosystem Governance and Management Body will be composed by a mix of public representatives (European Commission or a delegate), Member States and industry stakeholders' representatives involved in Plug & Charge related services. The participation in the group will be defined typically through the launch of a call for applications by the European Commission. The group will count with its corresponding Terms of Reference and Rules of Procedure.

6.2 E-mobility PKI Ecosystem Operating body

At the operational level of the EU PKI ecosystem for e-mobility, the Operating Body is responsible for running the elements required to achieve interoperability within the PKI ecosystem, with its PKI systems, through the CTL approach. This role should be covered by the European Commission or a delegate. The Commission may request the aid of external contractors selected via a tendering process in support of these activities (notably the procurement of ICT systems implementing the functions under the operational responsibility of the Commission). In that case, the Commission would ensure the lack of conflict of interest between organizations offering Plug & Charge services and organizations that would support the operation of the operating body and the CTL.

Procedurally, the Operating Body would be composed by the Trust List Manager, the e-Mobility Point of Contact (ePOC), and the Operations Manager.

- **Trust List Manager** (TLM): it represents the unique centralised role that holds the "TLM Certificate" used to sign the CTL. The TLM Certificate is the highest cryptographic certificate trust anchor. The TLM is responsible to update the CTL on the basis of the inputs of the so-called e-Mobility Point of Contact (ePOC), by including the newly accepted Root certificates as well as removing the expired and revoked ones.
- **e-Mobility Point of Contact** (ePOC): it collects applications from all operational Root CA certificates in the EU. Moreover, it publishes the CTL created by the TLM. It has therefore an external coordination role acting as an entry point for companies that want to apply for and or consult the CTL. It accepts or rejects the application of PKI Root operators to be included in the CTL and distributes the CTL.
- **Operations Manager**: it has an internal coordination role (opposed to the external coordination role of the ePOC). The main function includes the implementation of the operational requirements published by the Operation Governing Body, operating specific e-mobility infrastructure, and escalating incident reports to the Operation Governance Body. Specifically, it coordinates the operation of the system and interfaces with the stakeholders. It is the actor responsible for the organization of CTL signing sessions.

6.3 Independent Accredited PKI Auditors

In addition to the bodies described so far, for a functioning, secure and trustable e-Mobility Ecosystem a set of independent accredited PKI Auditors is needed to perform the auditing on Root CA operators (V2G, OEMs, and MOs). Specifically, the auditing body carrying out the audit shall be external and independent from the audited PKI system and accredited and certified by a member of European Accreditation against ISO 27001 and ISO 27006[27], or it shall be a

[27] ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

Technical Service accredited for UN Regulation 155[28] under EU Regulation 2018/858[29] (article 73). Each PKI System would be free to choose its independent accredited PKI Auditor.

Furthermore, the CTL, TLM, and ePOC will be subject to the same auditing obligation as any other PKI System. Also in this case, the PKI accredited auditor must be external and independent from the audited organizations. The European Commission will have to select and contract a suitable auditor to audit the elements of the ecosystem under its operational responsibility.

6.4 Market actors

The market actors are the entities that provide the PnC services at the operational level. Most notably in this category are included the PKI providers, OEMs, MOs, and CPOs among many others. The ePOC mediates the interaction among these actors and the European Governance. Market actors will run and participate in the existing PKI systems that will constitute the EU PKI ecosystem as reflected in Figure 1.

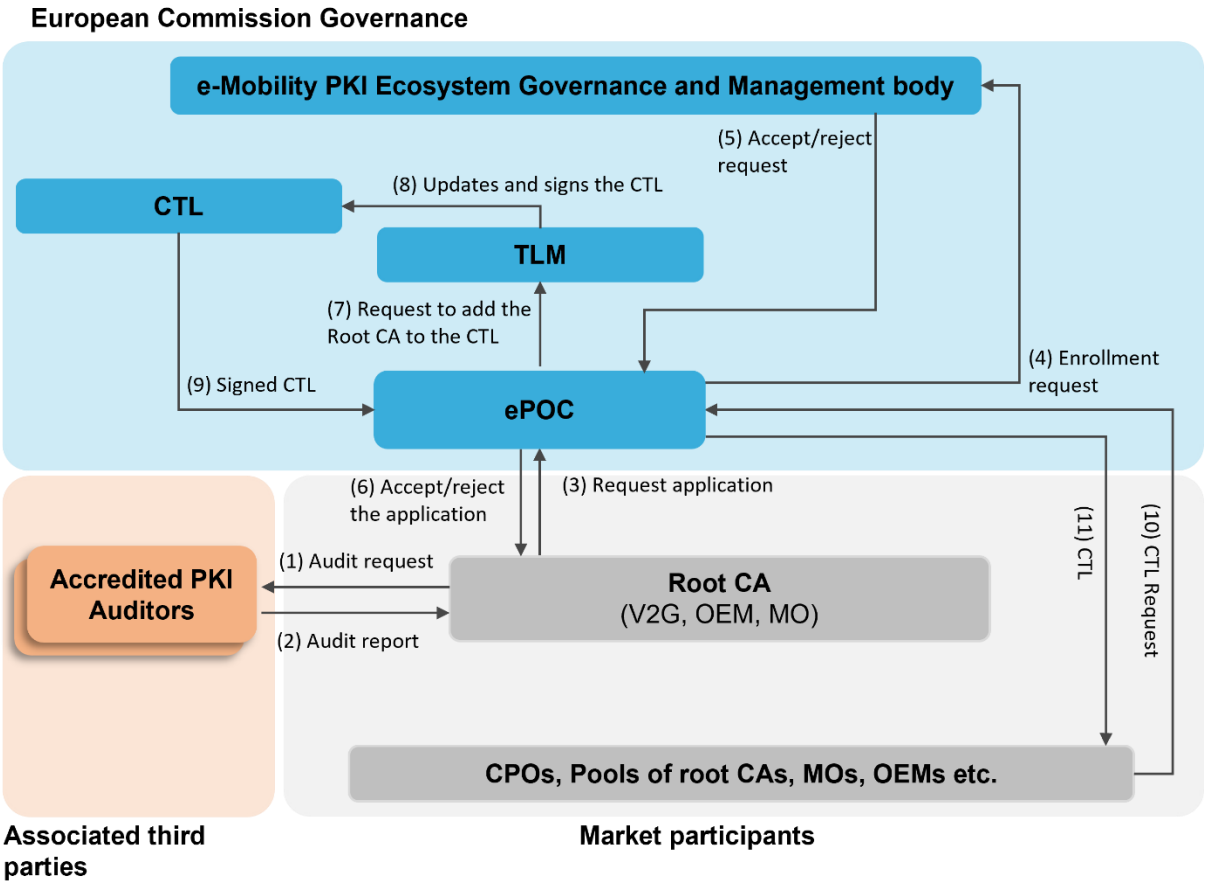
[28] UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system as published in the EU Official Journal [2021/387]. https://eur-lex.europa.eu/eli/reg/2021/387/oj

[29] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (Text with EEA relevance.). https://eur-lex.europa.eu/eli/reg/2018/858/oj

7 Operating model

The operating model is strictly linked to both the governance and architecture models (Chapters 5 and 6). It aims to capture the actors and the procedures involved in establishing and maintaining a governance based on the CTL approach for interoperability.

Figure 19: Operating model for the EU PKI for e-mobility



The operating model is subdivided into three areas:

1. **European Commission Governance** elements (blue box in Figure 19), including the e-Mobility PKI Ecosystem Governance body, the ePOC, the TLM and CTL.
2. **Market participants** (grey box Figure 19), composed by the PKI system with the Multi-Root CAs of different actor groups (V2G, OEM, and MO) which are entitled to have their own Root Certificates included in the CTL upon compliance with the requirements set out in the secondary legislation under AFIR for the EU PKI ecosystem. Additionally, in the same area are contained all those parties that would want to consult the CTL, this includes CPOs, Certificate Pools, MOs, OEMs, among many others.
3. **Associated third parties**, including the Accredited PKI Auditors (orange box in Figure 19).

The operating model flow is summarised in Table 15. The on-boarding process comprises of flows 1 to 6. It starts when a Root CA initiates the process to be included in the CTL, it needs to be audited by an Accredited PKI Auditor (see paragraph 6.3.). The Root CA sends an audit request to a selected Accredited PKI Auditor. After the auditors carries out the audit procedure defined by the ePEGMB, the results are sent back to the Root CA in the form of an audit report.

The Root CA can then proceed to file through the ePOC a request application to have its Root Certificate included in the CTL (flow 7). The request is composed by a set of forms available in the ePOC and the audit report. If the Root CA provided evidence of compliance to all the requirements, the ePOC sends and enrolment request to the ePEGMB. The latter inspects the audit report and the accreditation of the auditor and either accepts the request, or it can reject it if there are reasons to keep the Root CA outside the ecosystem regardless their eligibility against the aforementioned requirements. The ePOC then communicates the response (acceptance or rejection) of the Root CA request application. If the application is accepted, the ePOC sends to the TLM the corresponding certificate information to be integrated in the CTL. At the first available CTL signing session, the TLM will update the CTL including the new Root Certificates and removing all the expired and revoked ones. The updated CTL is signed with the TLM certificate and included in the ePOC. In this way, all the interested market parties can send a request to the ePOC to obtain the latest version of the CTL available. The market parties, in order to have the latest updated version of the CTL, shall set up a script sending to the ePOC a CTL request on a regular basis. The suggested timeframe is once per day but at the minimum once per week.

The table below provides a summary of the flow of the operating model.

Table 15: Summary of the operating model flow

Flow ID	From	To	Content	Type of communication
(1)	Root CA	Accredited PKI Auditor	Audit request	Org. to Org.
(2)	Accredited PKI Auditor	Root CA	Audit report	Org. to Org.
(3)	Root CA	ePOC	Request application to be included in the CTL	Org. to IT
(4)	ePOC	ePEGMB	Enrolment request for the Root CA that submitted a valid application	Org. to Org.
(5)	ePEGMB	ePOC	Accept/reject the enrolment request	Org. to Org.
(6)	ePOC	Root CA	Information about the acceptation of rejection of the application	IT to Org.
(7)	ePOC	TLM	Request to add the Root CA certificate information to the CTL	IT to IT
(8)	TLM	CTL	Update and sign the CTL with the new information	IT to IT
(9)	CTL	ePOC	The signed CTL is transmitted to the ePOC	IT to IT
(10)	Market participants	ePOC	Request of the updated CTL	IT to IT

(11)	ePOC	Market participants	CTL	IT to IT

Other potential aspects that would require further discussion or clarification in relation to the governance and architecture of the EU PKI ecosystem will be addressed by the European Commission together with industry stakeholders as part of the future *e-mobility PKI Ecosystem Governance and Management* body, which will function as an expert group of the European Commission.

EUROPEAN COMMISSION
Directorate-General for Mobility and Transport

Directorate B – Investment, Innovative & Sustainable Transport
B4 – Sustainable & Intelligent Transport

EUROPEAN COMMISSION SUPPORT STUDY

DEVELOPMENT OF A GOVERNANCE FRAMEWORK FOR THE EU PUBLIC KEY INFRASTRUCTURE (PKI) BASED ON THE STANDARD ISO 15118

DELIVERABLE 2 – RELEVANT STANDARDS AND TECHNICAL ASPECTS OF THE PKI TO ALLOW INTEROPERABILITY ACROSS V2G ROOT CAs

Objective: The aim of this deliverable is to elaborate in a compehensive manner **the required technical elements and standards to ensure interoperability for a future CTL architecture**. In particular, the document shall define on what governance and technical level this will be ensured, namely by who and how. To achieve this purpose, the concrete following elements are developed:

- Mapping of standards and protocols in view of a EU CTL architecture;
- Identificaiton of concrete standardisation gaps and determination of a way forward on how to address them in support of the PKI;
- Interoperability in the CTL architecture including the technical elements that need to be in place;
- Fitness for purpose of ISO 15118 (-2 and -20) for a CTL architecture including the missing elements and how to address them;

Importantly, this document aims also to help coordinate the standardisation activities and participation of interested stakeholders on the set-up and and offering of service through a potential European PKI based on a CTL architecture with a hybrid governance model (public/private).

Extension: To be discussed.

Foreword

This document is a deliverable in support of the preparation of secondary legislation (i.e. delegated and/or implementing acts) under the Alternative Fuels Infrastructure Regulation (AFIR)[30]. This concrete deliverable elaborates on the development of a governance, architecture, and implementation plan for the set-up and operation of an EU Public Key Infrastructure (PKI) ecosystem in the EU.

The document has been developed as part of the European Commission 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC. The document has also been reviewed and validated by the Sustainable Transport Forum (STF), which is established and chaired by the European Commission services since April 2015 to assist the Commission in implementing the Union's activities and programmes aimed at fostering the deployment of alternative fuels infrastructure to contribute to the European Union energy and climate goals.

The study was articulated in two phases.

Phase 1 of the 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC.

During the first phase, the study was centred around bilateral interviews with the existing PKI service providers and research projects of the Sustainable Transport Forum (STF) subgroup on Governance & Standards - namely CharIN, Gireve, Hubject, SAE, and Vedecom. The result of this phase has been the development of a set of recommendations on a high-level governance and architecture framework for the functioning and operation of a PKI ecosystem in the EU. These recommendations were later transmitted and reviewed by the STF sub-group on governance and standards, being those endorsed by the sub-group as part of the document *Activity 2 - 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*[31].

- **Recommendation 1: A regulated vs. non-regulated governance and architecture –** the STF sub-group favours a regulated approach for the governance and architecture in Europe due to the advantage of providing a clear legal basis covering key elements of the PKI.
- **Recommendation 2: Single or Multi Root CA model** - The STF sub-group members advocate for a multi-Root CA model due to the benefits of having competition in the market among several V2G Root CAs – increased variety and quality of service, reduced prices - as well as the increased operational resilience of the PKI. Also, this approach also supports the current market situation under which multiple market actors are already committed to offering the service of V2G Root CA in the EU.
- **Recommendation 3: Architecture model to ensure interoperability across Multi Root CAs** - the STF sub-group members' preferred interoperability solution across the multi-Root CA model is a Certificate Trust List (CTL), due to the solution's

[30] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1867

[31] https://op.europa.eu/en/publication-detail/-/publication/b7910659-276c-11ee-839d-01aa75ed71a1/language-en

potential for scalability, centralised maintenance, and fitting logic of certificate verification.

- **Recommendation 4: Governance Model –** the STF sub-group members on G&S prefer a mixed approach, involving both private and public stakeholders. The combination of categories of entities such as businesses organisation, industry consortia and public authorities allows to leverage the strengths of each of them while minimising the downsides.
- **Recommendation 5: Ownership model** – the STF sub-group members on G&S agree on having a central public authority (i.e. European Commission) to perform the governance roles of the PKI (i.e. Definition of criteria for Root CAs operators, check of the criteria, and distribution of the CTL) while the managing and operating layer of the multiple PKI systems (i.e. operations of the PKI and the actual provision of the emission of certificates and signing service) could be covered by a combination of business organisations, industry consortia and public authorities.
- **Recommendation 6: Implementation scheme for the proposed governance and architecture solution** – the STF sub-group members on G&S agree that the development of the preferred governance and architecture solution will most likely occur in two phases. The initial phase will see the continuing of the existing Plug & Charge service solutions with their corresponding PKI implementations where the market is further tested and scaled-up by market actors. This relates in particular to existing implementations of ISO 15118-2. The second phase will be based on a regulated approach by the European Commission under a set of governance and architecture rules applicable in the EU considering the elements developed in the deliverables of this study and the recommendations of the STF Sub-group. A future PKI ecosystem will consider existing implementations based on ISO 15118-2 and, at the same time, will transition towards a future based on ISO 15118-20.

Phase 2 of the 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC.

The second phase of the study builds on the recommendations of the previous phase. Specifically, a dedicated group of experts was specifically formed to work on the following set of deliverables aiming to define the policy, technical and governance elements to guide the set-up and develop a regulated approach to a Multi-Root CA model with the CTL as the preferred interoperability solution. All this, under a mixed (public/private) governance approach:

Table 16: List of deliverables completed under the Support Study

Deliverable	Title
1	**Deliverable 1** - Architecture, governance, and operating model for a PKI based on ISO 15118;
2	**Deliverable 2** - Relevant standards and technical aspects of the PKI to allow interoperability across V2G Root CAs;
3	**Deliverable 3** - Market rules for the EU PKI ecosystem for e-mobility;
4	**Deliverable 4** - Mutually recognised set of criteria for Root CAs, Subscribers and the CTL of the EU PKI ecosystem for e-mobility;

5	**Deliverable 5** - Implementation plan for the preferred governance and architecture model;

More specifically, the present deliverable is the result of the work of the working group coordinated under the European Commission 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC. The organisations comprising the working group are the following members of the STF subgroup on Governance & Standards:

- CharIN,
- Gireve,
- Hubject,
- SAE,
- Vedecom,
- ChargePoint,
- ElaadNL,
- EnBW,
- Shell,
- Smartlab,
- Tesla,
- E-clearing.net.

The work developed by the working group and reflected in these deliverables has been also subject to the review and validation of the Sustainable Transport Forum (STF) Sub-group on Governance & Standards.

Scope of Deliverable 2

The **purpose of this deliverable is to provide a robust analysis of the state of play of the existing standards/protocols**, identifying what is the current state of development, and what is the expected final outcome of the ecosystem in support of the EU PKI ecosystem. This deliverable also aims at providing clarity on the interaction between the different **standards/protocols** with the goal of identifying those gaps that need to be fulfilled.

1 Starting point: Relevant communication protocols and standards

The **Mapping of the discussion concerning standards and protocols for communication exchange in the electromobility ecosystem**[32] carried out by the **STF Sub-group on Governance & Standards** (hereinafter Sub-group) gathers a comprehensive overview of the state of play of communication standards in the electromobility ecosystem. In practice, four main areas of communication within the EV recharging ecosystem have been identified:

- Communication between EV-CP
- Communication between CP-CPO (back-end)
- Communication between CPO-EMSPs/e-roaming platforms
- Communication between CPO-Energy system (grid integration)

Activity 1 of the STF Sub-group aimed to bring clarity on the current state of development by international standardisation organizations as well as industry-driven activities. Therefore, the goal was to provide a comprehensive view of the current applications based on de jure and de facto standards, elaborating on the potential benefits of including in EU legislation de jure standards that converge the features of de facto standards. Conceptually, there are three types of protocols and standards of application:

- Standards (*de jure*) developed by recognized international and/or European standardization organizations (ISO, IEC, EN, etc.)
- Industry protocols/standards (*de facto*) - developed by industry associations and alliances, etc. (e.g. OCPP, OCPI, etc.)
- Proprietary protocols/standards – developed by private companies/consortia;

Activity 1 report allowed to conclude that there is work ongoing by international and European standardisation organisations to ensure coordination between ISO 15118 and other relevant de jure standards expected to govern and harmonize the communication between CP-CPO (IEC 63110), CPO-EMSPs/e-roaming platforms (IEC 63119). Similarly, there is work ongoing and application examples to ensure interoperability between ISO 15118 and other relevant de facto protocols/standards currently applied by the industry addressing the communication between CP-CPO (OCPP), CPO-EMSPs/e-roaming platforms (OCPI), CPO-grid (OpenADR)

Moving forward, **Activity 2 of the STF Sub-group** – *Development of a governance and architecture framework for the implementation and operation of a Public Key Infrastructure (PKI) ecosystem for e-mobility in the European Union* – aimed to deepen into this topic focusing on the high-level elements required for the development of a governance structure and implementation strategy for the operation of a PKI (Public Key Infrastructure) ecosystem.

In particular, **Block 3 of Activity 2**, provided a mapping of the different existing communication strands within the EV charging ecosystem, indicating the potential standards covering that area, as shown in the image below:

[32] https://op.europa.eu/en/publication-detail/-/publication/a8cd2c4b-54dc-11ed-92ed-01aa75ed71a1/language-en

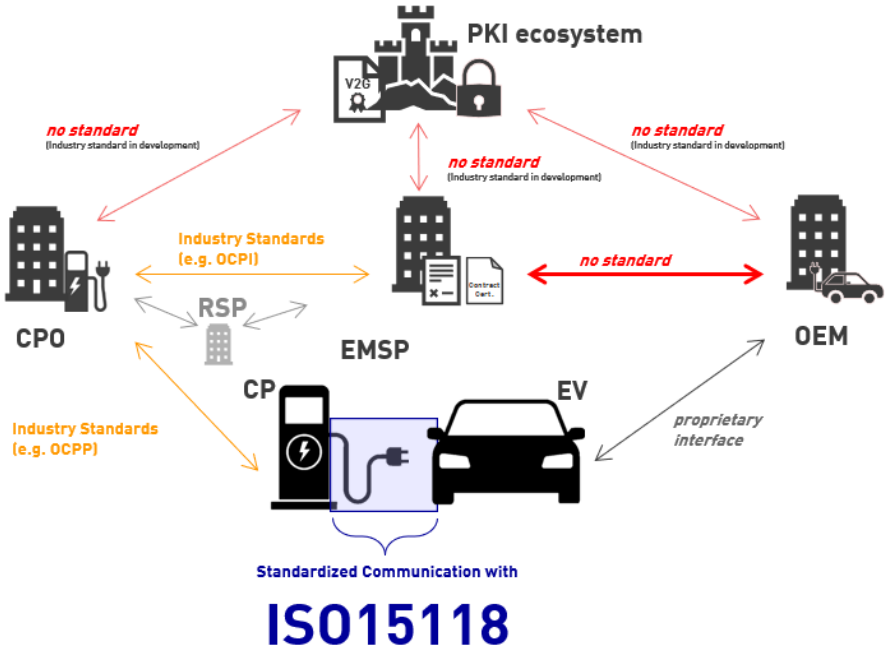


Figure 20: Visualization of the standardisation areas in the EV charging ecosystem and existing gaps

As shown in the figure, in addition to the lack or still developing phase of certain communication standards, there are a significant number of non-standardized processes yet in the ecosystem, including interoperability aspects in relation to a PKI implementation under a CTL architecture.

It is therefore **the purpose of this deliverable to provide a robust analysis of the state of play of this standard/protocols**, identifying what is the current state of development, who is participation and how, and what is the expected final outcome of the ecosystem in support of the EU PKI ecosystem.

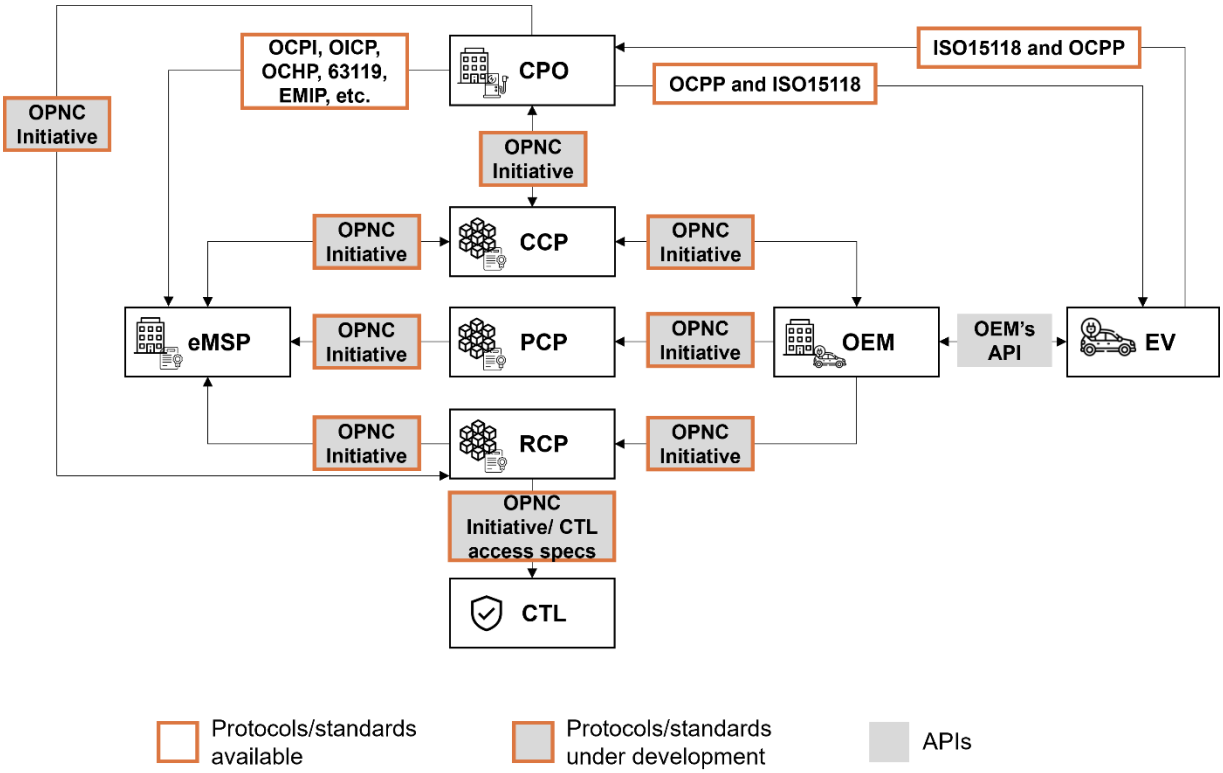
2 Identification of standardization gaps in support of the EU PKI governance and architecture

2.1 Working point 1 – Analysis of the different communication strands

In this section, using as a starting point the work carried by Block 3 of Activity 2, it has been carried out an analysis of the different communication strands with a focus on ensuring communication and interoperability of the PKI governance and architecture (based on a CTL with a hybrid governance approach).

The image below illustrates the existing standards and protocols that allow the communication between the different actors in the PKI ecosystem.

Figure 21: Overview of the protocols in the EU PKI Ecosystem for e-Mobility



The table below describes in further detail the different types of communication, highlighting when protocols and standards are present or are missing.

Table 17: Listing of the principal communication lines related to the Plug and Charge use case

#	Stakeholder (Communication from)	Reason behind communication (High level use case)	Communication to whom	Standards and protocols to use	Who does what?
1	OEM	Making available provisioning certificates to EMSP	PCP: "Provisioning Certificate Pool"	OPNC	OPNC task force within CharIN
2	OEM	Obtaining the V2G Root Cas Certificate to be installed in EVs	Root certificate pool (preferable)	OPNC	OPNC task force within CharIN
3	EMSP	Request PC (provisioning certificate) with PCID to enable the creation of CC (contract certificate)	PCP: "Provisioning Certificate Pool"	OPNC	OPNC task force within CharIN

#	Stakeholder (Communication from)	Reason behind communication (High level use case)	Communication to whom	Standards and protocols to use	Who does what?
4	EMSP	Access CTL to check OEM root and verify provisioning certificate	Root certificate pool	OPNC	OPNC task force within CharIN
5	Root certificate pool	Root certificate pool access the CTL from the ePOC	CTL	OPNC / CTL access specs	OPNC task force within CharIN
5	EMSP or CProvS	Making contract certificates available in the pools for OEMs and/or CPOs.	Contract Certificate Pool	OPNC	OPNC task force within CharIN
6	Contract Certificate Pool	Obtaining the Contract Certificate to be installed in the EVs	OEMs	OPNC	OPNC task force within CharIN
7	Contract Certificate Pool	Obtaining the Contract Certificate to be installed in the EVs	CPO	OPNC	OPNC task force within CharIN
8	OEMs	Installing the Root CAs	EV	Proprietary OEM's API	No action needed
9	OEMs	Provision of the contract certificates in the EV	EV	Proprietary OEM's API	No action needed
10	EV	When CC installation goes via Charging Station and the notification about an available CC has been received: EV sends installation request using a PCID	CPO	ISO 15118 from EV to EVSE, OCPP from EVSE to CPO	ISO / OCPP / IEC 63110

#	Stakeholder (Communication from)	Reason behind communication (High level use case)	Communication to whom	Standards and protocols to use	Who does what?
11	CPO	CPO retrieves CC to be installed in the EV via the charger	EV	First OCPP from CPO to EVSE, then ISO 15118 form EVSE to EV	ISO / OCPP / IEC 63110
12	EV	EV informs OEM about the status of the contract certificate (i.e., installation, revocation, etc.)	OEM	Proprietary OEM's API	No action needed
13	OEM	OEM informs Pools about the status of the contract certificate (i.e., installation, revocation, etc.)	Contract Certificate Pools	OPNC	OPNC task force within CharIN
14	EV	EV informs CPOs about the status of the contract certificate (i.e.,, installation, revocation, etc.)	CPOs	ISO 15118 from EV to EVSE, then OCPP from EVSE to CPO	ISO / OCPP task force
15	CPOs	CPO inform Pools about the status of the contract certificate (i.e.,, installation, revocation, etc.)	Contract Certificate Pools	OPNC	OPNC task force within CharIN
16	Contract Certificate Pool	Contract Certificate Pools informs EMSP about successful installation in the EV	EMSP	OPNC	OPNC task force within CharIN
17	EV	EV is plugged into the charger, PnC preconditions are fulfilled. CC of any PKI is transferred to the charger and ultimately the	CPO and Charge Point	ISO15118 form EV to EVSE, then OCPP from EVSE to CPO	ISO / OCPP / IEC 63110

#	Stakeholder (Communication from)	Reason behind communication (High level use case)	Communication to whom	Standards and protocols to use	Who does what?
		CPO			
18	CPO	Obtaining the MO Root Cas to be used for Contract Certificate validation	Root certificate pool (preferable)	OPNC	OPNC task force within CharIN
19	CPO	CPO requests authorisation from EMSP via Roaming.	EMSP	OCPI OICP OCHP 63119 EMIP …	Organisation/bodies/working groups in charge of the protocols.
20	CPO	Start Energy Transfer after positive result of (17)	EV	ISO 15118	No action needed

The CTL can be accessed by the actors of the European PKI Ecosystem for e-Mobility indirectly through the Certificate Pools (as outlined in the table), or directly with any mean available. The table above covers the former option, as it is the recommended approach. To make the latter approach feasible, the European PKI Ecosystem Governance and Management Body (EPEGMB) would have to set up a dedicated set of APIs to enable the ecosystem participants to directly access the CTL.

2.2 Working point 2 – Areas of further elaboration

Table 17 above described in detail the different types of communication, highlighting when protocols and standards are present or are missing. Based on the analysis carried out, it was identified a set of standardisation elements that need to be further elaborated. More specifically, these are some standardization areas that, either:

1) Require further harmonization and convergence,
2) Need to be harmonized at international/European level in support of the PKI,
3) Require a standard not covered by existing standards and/or protocols.

A breakdown of each standard/protocol featured in the table above is provided below, to highlight their development status while identifying a path for further development in line with the future EU PKI ecosystem.

ISO 15118

The standard ISO 15118 covers the communication between EVs and EVSEs. The standard - with its Part 20 - does not require any further structural development for the implementation of the Plug and Charge use case. The only addition that could be highly beneficial for the sake of the proposed governance and architecture for the European PKI Ecosystem for e-mobility is a formal integration of the CTL. This standardization scenario, along with other possible ones, is explained in "Deliverable 5 – Development of an implementation plan for the preferred governance, architecture and operating model" of the support study.

Protocol under the Open Plug and Charge (OPNC) Taskforce

The OPNC taskforce in CharIN is currently developing a protocol which covers the relevant communication aspects for Plug and Charge involving relevant participant actors (i.e., OEMs, CPOs, and EMSPs, etc) and including the Certificate Pools (CCP, PCP, RCP) and *vice versa*. The aim of the taskforce is to finalise the protocol by the end of 2023. Upon the formal implementation of the European Commission governance under the form of the EPEGMB, it has been agreed that the Commission or a delegate (i.e., JRC) will be granted access to the OPNC taskforce to monitor the protocol development, contribute to its evolution as well as initiating the discussion for its formal adoption through a standardisation organisation.

OCPP

The Open Charge Point Protocol (OCPP) is being developed by the Open Charge Alliance (OCA) and aims to be a free open-source protocol to support communication between a charge point and a management system. Similarly to the previous protocol, the Commission or a delegate (i.e., JRC) would be granted access to the OCPP working group to monitor the protocol development, and contribute to its evolution and potential contribution to the EU PKI ecosystem.

At the moment of finalising this report (July 2023), the European Commission together with CEN-CENELEC are moderating a discussion between OCA and IEC 63110 in order to ensure the convergence of OCPP and IEC 63110, thus, having one single international standard with a common governance process and a certain future development process that takes into account the European Commission needs and request in line with the relevant standardisation requests[33].

CTL technical specifications

Given the preferred solution for governance and architecture of the European PKI Ecosystem for e-Mobility involves the set-up and operation of a CTL, the European Commission or a delegate (i.e., JRC) needs to set up a series of technical specifications to allow any ecosystem participant (and the Certificate Pools in particular) to directly access the CTL. The European Commission, in agreement with industry stakeholders, will ensure the development of such specifications, including the adoption of a European standards to this end in complementarity with the OPNC protocol.

In the C-ITS domain, the European Commission has already in collaboration with ETSI supported the development of existing technical specifications for the EU C-ITS security PKI. These are listed below, and represent a good reference for the work on the technical specifications for the EU PKI for e-mobility.

[33] Mandate M-581 https://ec.europa.eu/transparency/documents-register/detail?ref=C(2022)1710&lang=en

- ETSI TS 102 941, Intelligent transport systems (ITS) – security, trust and privacy management.
- ETSI TS 102 940, Intelligent transport systems (ITS) – security, ITS communications security architecture and security management
- ETSI TS 102 042 Policy requirements for certification authorities issuing public key certificates.
- ETSI TS 103 097 Intelligent transport systems (ITS) – security, security header and certificate formats

OEMs' proprietary APIs

At present, each OEM typically develops its set of proprietary APIs to enable communication between its backhand and each EV. These APIs are out of scope for the purpose of this document as their development is the sole responsibility of each OEM.

Importantly, the in-vehicle interface with the EV driver should provide an open and user-friendly channel to enable the driver to pick alternative service providers to prevent vendor lock-in effects for essential services such as certificate installation, including the OEM proprietary API's themselves if are not working or are not desired by the EV driver. The European Commission, in the context of the access to in-vehicle data initiative is expected also to address this aspect (e.g., potential revision of EU type approval legislation), thus, ensuring that the relevant resources and functionalities are available for the implementation of these solutions.

Other protocols

The residual protocols used for the communication between CPOs and EMSPs (OCPI, OICP, OCHP, EMIP) can be further expanded in autonomy by the organisations that initially developed them. The EPEGMB would have to monitor the novel modification to all the relevant protocols to ensure an appropriate oversight of the ecosystem.

It is a declared objective of the European Commission to support interoperability and market simplification, by ensuring the involved industry actors work together converge existing solutions.

3 Listing and definition of relevant standards and protocols

Below is provided a concise summary description of each standard/protocol with relevance to the EU PKI ecosystem for e-mobility in a greater or lesser extent:

ISO 15118 facilitates communication between the EV and the EVSE. It sends charging parameters based on user needs and the charging profiles from the CPO. The latest Part 20 includes protocols for bidirectional charging.

IEC 61850 is a group of standards defining communication protocols for intelligent electronic devices at substations. It is a foundational standard for smart grids.

IEC 63110 is protocol for management of electric vehicles charging and discharging infrastructures. Current IEC 63110-1:2022 serves as a basis for the other future parts of IEC 63110, covering the definitions, use cases and architecture for the management of electric vehicle charging and discharging infrastructures. It addresses the general requirements for the establishment of an e-mobility ecosystem, therefore covering the communication flows between different e-mobility actors as well as data flows with the electric power system. The European Commission is currently supporting discussion for a convergence of OCPP and IEC 63110.

IEEE 2030.5 enables utility management of distributed energy resources, such as electric vehicles, through demand response, load control and time-of-day pricing. **Open Charge Point Protocol** (OCPP) communicates smart charging features, such as grid capacity, energy prices, local supply of sustainable energy, and user preferences. It is currently being incorporated into IEC 63110 to establish a regular international technical standard.

Open Charge Point Protocol (OCPP) communication protocol for networked electric vehicle chargers. The goal of OCPP is to make EV chargers work with EV charging management software.

Open Charge Point Interface (OCPI) supports connections between electric mobility service providers and CPOs, allowing EV users to access different charging points and streamline payments across jurisdictional borders. This helps support EV uptake through roaming. OCPI supports the most functionalities, including smart charging, among different roaming protocols. It is commonly used in the European Union.

Open Automated Demand Response (OpenADR) communicates price and event messages between the utility and connected distributed energy resources for the purpose of demand-side management. It focuses on exchanging information, whereas OCPP has more emphasis on control. OpenADR 2.0b has received approval as IEC Standard in 2019.

Open Smart Charging Protocol (OSCP) communicates predictions of locally available capacity to charging station operators. The current version contains use cases with more generic terms to allow integration of solar PVs, batteries and other devices. However, the use of OSCP is still limited.

EUROPEAN COMMISSION
Directorate-General for Mobility and Transport

Directorate B – Investment, Innovative & Sustainable Transport
B4 – Sustainable & Intelligent Transport

EUROPEAN COMMISSION SUPPORT STUDY

DEVELOPMENT OF A GOVERNANCE FRAMEWORK FOR THE EU PUBLIC KEY INFRASTRUCTURE (PKI) BASED ON THE STANDARD ISO 15118

DELIVERABLE 3 – MARKET RULES FOR THE EU PKI ECOSYSTEM FOR E-MOBILITY

Objective: The aim of this deliverable is **to capture the consensus between EU market actors on the definition of market rules** for the e-mobility PKI in the EU.

The activity builds on the work carried out by the participant members of the working group set up and coordinated under the European Commission Support Study.

Extension: To be discussed.

Foreword

This document is a deliverable in support of the preparation of secondary legislation (i.e., delegated and/or implementing acts) under the Alternative Fuels Infrastructure Regulation (AFIR)[34]. This concrete deliverable elaborates on the development of a governance, architecture, and implementation plan for the set-up and operation of an EU Public Key Infrastructure (PKI) ecosystem in the EU.

The document has been developed as part of the European Commission 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC. The document has also been reviewed and validated by the Sustainable Transport Forum (STF), which is established and chaired by the European Commission services since April 2015 to assist the Commission in implementing the Union's activities and programmes aimed at fostering the deployment of alternative fuels infrastructure to contribute to the European Union energy and climate goals.

The study was articulated in two phases.

Phase 1 of the 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC.

During the first phase, the study was centred around bilateral interviews with the existing PKI service providers and research projects of the Sustainable Transport Forum (STF) subgroup on Governance & Standards - namely CharIN, Gireve, Hubject, SAE, and Vedecom. The result of this phase has been the development of a set of recommendations on a high-level governance and architecture framework for the functioning and operation of a PKI ecosystem in the EU. These recommendations were later transmitted and reviewed by the STF sub-group on governance and standards, being those endorsed by the sub-group as part of the document *Activity 2 - 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*[35].

- **Recommendation 1: A regulated vs. non-regulated governance and architecture –** the STF sub-group favours a regulated approach for the governance and architecture in Europe due to the advantage of providing a clear legal basis covering key elements of the PKI.
- **Recommendation 2: Single or Multi Root CA model** - The STF sub-group members advocate for a multi-Root CA model due to the benefits of having competition in the market among several V2G Root CAs – increased variety and quality of service, reduced prices - as well as the increased operational resilience of the PKI. Also, this approach also supports the current market situation under which multiple market actors are already committed to offering the service of V2G Root CA in the EU.
- **Recommendation 3: Architecture model to ensure interoperability across Multi Root CAs** - the STF sub-group members' preferred interoperability solution across the multi-Root CA model is a Certificate Trust List (CTL), due to the solution's potential for scalability, centralised maintenance, and fitting logic of certificate verification.

[34] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1867

[35] https://op.europa.eu/en/publication-detail/-/publication/b7910659-276c-11ee-839d-01aa75ed71a1/language-en

- **Recommendation 4: Governance Model –** the STF sub-group members on G&S prefer a mixed approach, involving both private and public stakeholders. The combination of categories of entities such as businesses organisation, industry consortia and public authorities allows to leverage the strengths of each of them while minimising the downsides.
- **Recommendation 5: Ownership model** – the STF sub-group members on G&S agree on having a central public authority (i.e. European Commission) to perform the governance roles of the PKI (i.e. Definition of criteria for Root CAs operators, check of the criteria, and distribution of the CTL) while the managing and operating layer of the multiple PKI systems (i.e. operations of the PKI and the actual provision of the emission of certificates and signing service) could be covered by a combination of business organisations, industry consortia and public authorities.
- **Recommendation 6: Implementation scheme for the proposed governance and architecture solution** – the STF sub-group members on G&S agree that the development of the preferred governance and architecture solution will most likely occur in two phases. The initial phase will see the continuing of the existing Plug & Charge service solutions with their corresponding PKI implementations where the market is further tested and scaled-up by market actors. This relates in particular to existing implementations of ISO 15118-2. The second phase will be based on a regulated approach by the European Commission under a set of governance and architecture rules applicable in the EU considering the elements developed in the deliverables of this study and the recommendations of the STF Sub-group. A future PKI ecosystem will consider existing implementations based on ISO 15118-2 and, at the same time, will transition towards a future based on ISO 15118-20.

Phase 2 of the 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC.

The second phase of the study builds on the recommendations of the previous phase. Specifically, a dedicated group of experts was specifically formed to work on the following set of deliverables aiming to define the policy, technical and governance elements to guide the set-up and develop a regulated approach to a Multi-Root CA model with the CTL as the preferred interoperability solution. All this, under a mixed (public/private) governance approach:

Table 18: List of deliverables completed under the Support Study

Deliverable	Title
1	**Deliverable 1** - Architecture, governance, and operating model for a PKI based on ISO 15118;
2	**Deliverable 2** - Relevant standards and technical aspects of the PKI to allow interoperability across V2G Root CAs;
3	**Deliverable 3** - Market rules for the EU PKI ecosystem for e-mobility;
4	**Deliverable 4** - Mutually recognised set of criteria for Root CAs, Subscribers and the CTL of the EU PKI ecosystem for e-mobility;
5	**Deliverable 5** - Implementation plan for the preferred governance and

	architecture model;

More specifically, the present deliverable is the result of the work of the working group coordinated under the European Commission 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC. The organisations comprising the working group are the following members of the STF subgroup on Governance & Standards:

- CharIN,
- Gireve,
- Hubject,
- SAE,
- Vedecom,
- ChargePoint,
- ElaadNL,
- EnBW,
- Shell,
- Smartlab,
- Tesla,
- E-clearing.net.

The work developed by the working group and reflected in these deliverables has been also subject to the review and validation of the Sustainable Transport Forum (STF) Sub-group on Governance & Standards.

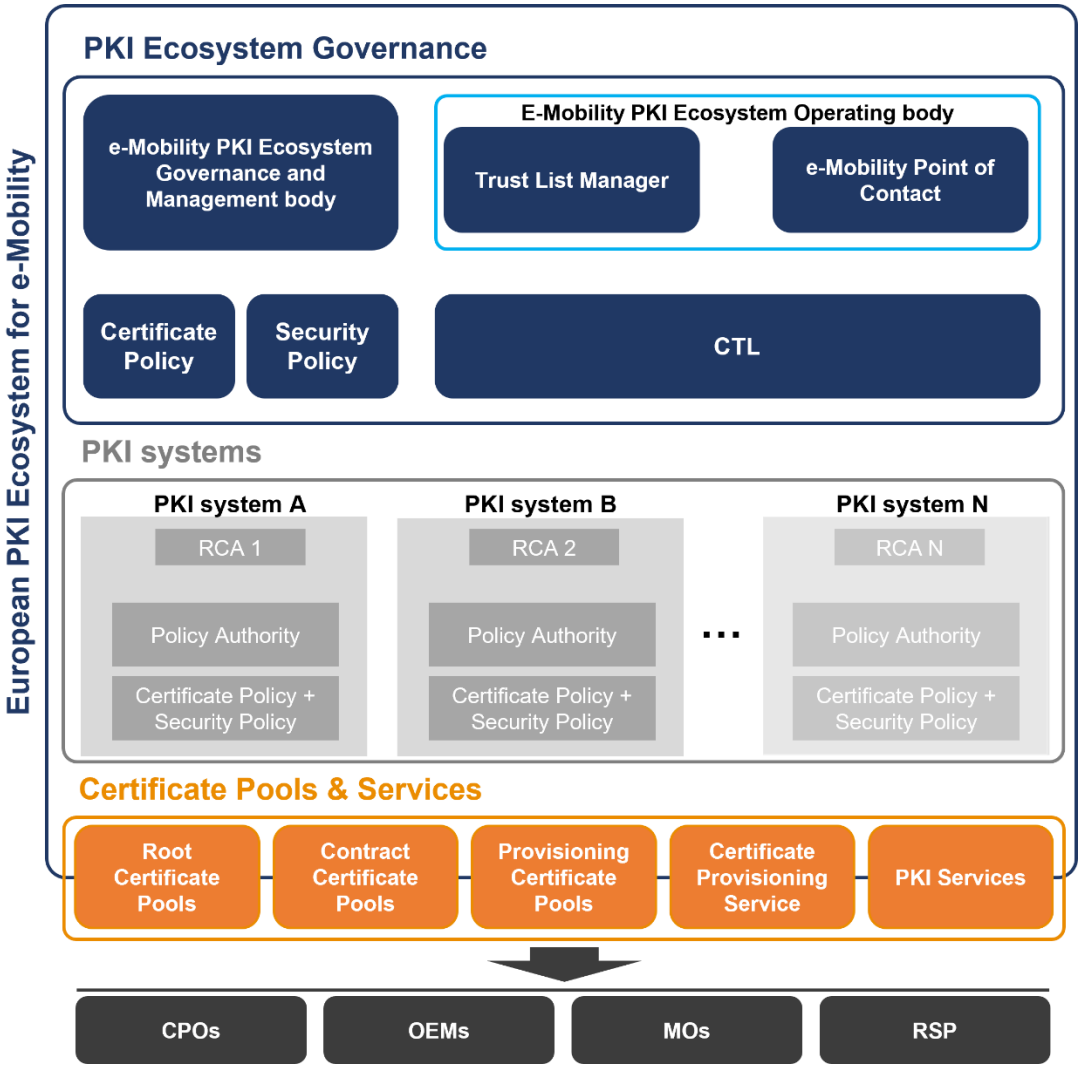
Scope of Deliverable 3

The **purpose of this deliverable is to develop a set of market rules for each potential category of actor identified with a meaningful role in the EU PKI Ecosystem for e-mobility**. The main goal is to ensure fairness, openness and a level playing field for all the ecosystem participants supported by common onboarding guidelines.

1 Introduction

For the elaboration of the market rules presented in this document it has been considered the EU PKI governance and architecture design as presented in Deliverable 1 and shown in the following figure.

Figure 22: Graphic representation of the EU PKI ecosystem



The market rules elaborated and described in this document are structured as follows:

1) Market rules for the EU PKI Ecosystem for e-mobility landscape.
2) Market rules for PKI Systems.
3) Market rules for Pools and Services.
4) Market rules for PKI participants.

In addition to these market rules, this deliverable also concerns the development of guidelines for:

1) Onboarding of PKI participants to a PKI system (Root CA).
2) Onboarding of a PKI system to the EU PKI ecosystem.

2 Main principles

The list that follows contains the main principles of the EU PKI Ecosystem for e-mobility, which are reflected in the market rules of this document.

The main principles of the EU PKI Ecosystem are:

1) The EU PKI Ecosystem for e-mobility is made up by one single governing and management body with full control and mandate to onboard, offboard PKI operators within the ecosystem. This is the role of the EU PKI Ecosystem Governing and Management body (EPEGMB).
2) The EU PKI Ecosystem consists of multiple PKI systems, each with a Root CA.
3) A PKI system can be shared or dedicated.
4) A Root CA needs to be accredited by the European Commission's governance authority.
5) Every accredited Root CA will be operated and maintained by and within each PKI system.
6) There are no limitations in the number of PKI systems operating in the EU PKI ecosystem, unless otherwise determined by the EU PKI Ecosystem Governing and Management body.
7) The PKI systems shall necessarily interact with the European Certificate Trust List (EU-CTL).
8) The European Commission is responsible to operate the EU CTL via a Trust List Manager (TLM).
9) The European Commission is responsible for the accreditation, onboarding and auditing process of every PKI system and Root CA.
10) The market is responsible to operate the PKI systems and provide services to the end users.

3 Market rules

The following sections cover the market rules for the PKI Ecosystem (section 3.1), the PKI system (section 3.2), the Pools and Services (section 3.3), as well as the PKI participants (section 3.4).

3.1 Market rules for the EU PKI Ecosystem for e-mobility

The paragraphs below address the market rules for the essential elements of the European Commission Governance for the European PKI Ecosystem for e-mobility.

3.1.1 European PKI Ecosystem Governing and Management Body (EPEGMB)

1) Accreditation of every Root CA of each PKI system is required by the EPEGMB. In order to be accredited, every Root CA shall present to the EPEGMB an audit report by an independent PKI accredited auditor consisting of:

- Declaration of successful onboarding.
- Declaration of compliance of the Root CA certificate policy with the “mutually recognised set of criteria for V2G Root CAs and sub-CAs, and minimum requirements for the certificate policy”.
- 100% score on all audit checks.

2) The EPEGMB is mandated to:
   - Supervise the onboarding according to the onboarding guidelines.
   - Check the compliance (using the audit reports) of the Root CAs to the set of minimum requirements to be considered a trustworthy Root CA operator.
   - Check the initial and periodical audit reports of the Root CA and PKI Providers performed by and independent PKI accredited auditor.
3) To be accredited, the PKI provider has to comply with the accreditation rules:
   - Submission of Certificate Policy.
   - Submission of Security Policy.
   - Comply with the periodic audit obligation, ensuring that audits are carried by an independent PKI accredited auditor and submitting the audit reports to the EPEGMB.
4) The EPEGMB is empowered to define potential additional criteria for the accreditation process based on the legal requirements established under the AFIR implementing act on the EU PKI ecosystem.
5) The PKI policy authority is required to publish policies and procedures for accreditation. Operators onboarded in the PKI Ecosystem for e-mobility which do not comply to the rules set out by the EPEGMB can be off-boarded by the EPGMB.
6) The PKI system operators shall choose and appoint an independent PKI accredited auditor to execute periodic audits and the first audit during onboarding. The auditor shall be required to supply a copy of its PKI accreditation as an annex to the audit reports.
7) Pricing and access to the EU PKI Ecosystem, including the services provided by PKI systems to the end users (e.g., Plug & Charge), shall be reasonable, easily and clearly comparable, transparent and non-discriminatory. Where relevant, prices and access levels may only be differentiated proportionately according to an objective justification.
8) The EPEGMB is responsible for updating the market guidelines and rules for the EU PKI ecosystem.

3.1.2 European Certificate Trust List (EU CTL)

1) Within the EU PKI Ecosystem, only one single Certificate Trust List (CTL) established by the European Commission shall interact with all accredited PKI systems containing all the root certificates from onboarded Root CAs, and the Trust List Manager will sign it.
2) If a Root CA is not fulfilling or no longer fulfilling the defined onboarding rules as per audit report, it will not be admitted and would be offboarded from the CTL as part of the EU PKI ecosystem for e-mobility.
3) The CTL established by the European Commission will be the mechanism to achieve interoperability with other PKI Ecosystems outside of the EU.
4) The CTL established by the European Commission will be published on a publicly accessible website to make the CTL available to any stakeholder.

3.1.3 European PKI Ecosystem Operating Body (EPEOB)

1) Within the EU PKI Ecosystem for e-mobility, there is one PKI Ecosystem Operating body (EPEOB), assigned and mandated by the EPEGMB.
2) The PKI Ecosystem Operating body is responsible for:
   - Assigning and mandating the TLM through a tendering process (system and operating entity);
   - Assigning and mandating the Operations Manager;
   - Assigning, mandating, and setting up the ePOC.

3.1.4 European Trust List Manager (EU TLM)

1) Within the EU PKI Ecosystem for e-mobility, one Trust List Manager is assigned and mandated by the PKI Ecosystem Operating body.
2) The TLM is role operated by an independent entity. Both system and operating entity comply with the rules and specifications outlined by the EPEGMB.
3) The TLM signs the CTL.
4) The TLM is responsible for updating the CTL based on the inputs of the e-mobility Point of Contact (EPOC), by including the newly accepted Root certificates and removing the expired and revoked ones.
5) The TLM is subject to the same auditing procedure of the Root CA performed by an independent PKI accredited auditor selected by the EPEGMB.

3.1.5 European PKI Ecosystem Operations Manager (EPEOM)

1) Within the EU PKI Ecosystem for e-mobility, there is one PKI Ecosystem Operation Manager is assigned and mandated by the EPEGMB.
2) The EPEOM shall plan regular CTL signing sessions according to the rules defined by the EPEGMB.
3) The EPEOM shall plan ad hoc CTL signing sessions/updates to deal with emergencies such as the revocation of Root certificates.
4) The EPEOM is responsible for coordinating the publication of the newly issued CTL.
5) The EPEOM is responsible for communicating the requests received through the ePOC to the EPEGMB for compliance assessment and onboarding decisions.

3.1.6 E-mobility Point of Contact (ePOC)

1) Within the EU PKI Ecosystem for e-mobility, there is one ePOC, assigned and mandated by the EU PKI ecosystem operating body.
2) The ePOC is responsible for:
   i. Handling onboarding applications of PKI participants, the ePOC forwards them to the EPEGMB for evaluation,
   ii. Maintaining an overview of trusted root CAs and active PKI participants,
   iii. Receiving and performing administrative and technical checks of requests from onboarded PKI participants (i.e., rekey and revocation requests). Accepted requests will be forwarded to the TLM for implementation,

iv. Communicating the acceptance or rejection of a request,
v. Publication of the CTL.

3.2 Market rules for PKI Systems

The paragraphs below address the market rules for shared and dedicated PKI systems, the PKI operators, and the PKI System and Ecosystem onboarding.

3.2.1 Root CAs in a PKI system

1) Any PKI system may consist of:
   i. a *dedicated* Root CA used by one PKI participant.
   ii. a *shared* Root CA used by several PKI participants, where access to the Root CA is determined by the owner of that PKI system.
2) Every Root CA (V2G, OEM and EMSPs) as part of a PKI system must be accredited by an independent PKI accredited auditor. The EPEGMB receives the audit reports and uses them to assess compliance.
3) Every Root CA shall be audited annually by an independent PKI accredited auditor of its choice and in line with requirements established under AFIR implementing act to this respect. The auditor shall be required to declare conformity based on international standards and European quality, security and certification requirements as defined by the EPEGMB.
4) All eligible Root CAs shall comply with international standards and European quality, security and certification requirements for PKI implementations as defined by the EPEGMB and in line with requirements established under AFIR implementing act to this respect.
5) All Root CAs minimum requirements related to security are determined in the PKI Certificate Policy (CP) and detailed in the Certification Practice Statement (CPS).
6) All Root CA minimum requirements related to business and market rules are defined in the onboarding guidelines and will be accepted by PKI participants prior to onboarding.
7) The PKI provider is responsible to ensure interoperability. Concretely, any PKI system offering services in the EU shall necessarily be interoperable with other PKI systems within the EU PKI for e-mobility via the CTL mechanism.
8) Any PKI system is required to follow the communication requirements established by the EU PKI ecosystem operating body.

i. Dedicated PKI systems (single used Root CA)

1) Any dedicated PKI system shall comply with the rules outlined for Root CAs in a PKI system (section 3.2.1), and more generally, with all rules related to the EU PKI Ecosystem.
2) Any dedicated PKI system is used and maintained by a single PKI participant centred around a (V2G) Root CA operated by the same PKI participant. The PKI participant (EV-OEM, CP-OEM, EMSP or CPO) acts as a PKI provider without offering PKI services to other PKI participants. Thus, a dedicated PKI system does not need to onboard other PKI participants.

3) Pricing of any dedicated PKI system, including services offered to the end user, shall be reasonable, easily and clearly comparable, transparent and non-discriminatory. Where relevant, prices may only be differentiated proportionately according to an objective justification.

ii. Shared PKI systems (shared Root CA)

1) Any shared PKI system shall identify, thus, nominate a PKI provider to operate the shared Root CA.
2) The PKI provider nominated to operate the Root CA must comply with the rules outlined for Root CAs in a PKI system (section 3.2.1), and more generally, with all rules related to the EU PKI ecosystem.
3) Pricing and access to any shared PKI system, including services offered to the end user, shall be reasonable, easily and clearly comparable, transparent and non-discriminatory. Where relevant, prices and access levels may only be differentiated proportionately according to an objective justification.

3.2.2 PKI provider (operator)

1) Any PKI provider is subjected to a compliance audit according to the EPEGMB requirements. Periodical audits may follow the initial audit.
2) Any PKI provider is fully responsible for the PKI operations of their own Root CA(s).
3) Any PKI provider is fully responsible for collaboration in the ecosystem pool management services and interactions with the EU PKI ecosystem for e-mobility in line with the relevant rules and legal requirements established under the AFIR implementing act.
4) Any PKI provider may offer different types of Root CA services (i.e., V2G, OEM, or MO, etc.), however, any given Root CA shall be dedicated to one specific purpose.
5) The PKI provider is responsible for the Root CA operation and the Root CA interaction with the CTL of the EU PKI ecosystem for e-mobility.

3.2.3 Onboarding of a PKI system to the PKI Ecosystem

1) The onboarding of a given PKI system in the EU PKI Ecosystem for e-mobility necessarily implies the onboarding in the CTL established by the European Commission.
2) The EU PKI ecosystem is responsible to monitor and ensure that every PKI system implements the market rules and onboarding guidelines for the EU PKI Ecosystem for e-mobility, in line with the applicable rules and legal requirements established under AFIR delegate/implementing act and the future EU PKI Ecosystem Governing and Management body.
3) If at any time a new candidate PKI system is not fulfilling the onboarding rules due to the auditing process, it will not be onboarded in the PKI Ecosystem and CTL.
4) If at any time a PKI system already included in the EU PKI ecosystem for e-mobility is no longer fulfilling the onboarding rules as a result of the auditing, it will be offboarded from the EU PKI ecosystem and the CTL within a maximum time of two months (in line with the implementation and onboarding times of existing PKI participants to other PKI systems).

5) Any certificate issued by an offboarded PKI system, or any PKI system in general that does not follow the market rules and legal requirements of the EU PKI ecosystem, becomes automatically untrusted and shall be removed by any certificate pools.

3.2.4 Onboarding to a Shared PKI System

The onboarding rules listed in 3.2.3 are exclusively for shared PKI systems, and do not include dedicated PKI systems as those do not onboard other market participants.

1) The PKI provider shall ensure that every PKI participant agrees with the Certificate Policy, Security Policy, and the applicable rules contained in the Market and Onboarding Guidelines for the European E-mobility ecosystem.
2) The PKI provider of a shared PKI system shall ensure a fair and non-discriminatory onboarding of PKI participants to their own PKI system.
3) Any PKI provider shall publish all necessary onboarding documents and membership requirements to provide equal non-discriminatory access to every PKI participant.
4) If any new PKI participant is not fulfilling the onboarding rules, it will not be onboarded in the PKI system.
5) If an existing PKI participant is no longer fulfilling the onboarding rules, it will be offboarded from the PKI system within a maximum period of 2 months (with respect to the PKI participant).

3.3 Market rules for Pools and Services

The following sub-sections cover the market rules for Certificate Pools and PKI Services which are required for a smooth functioning of the EU PKI Ecosystem for e-mobility and individual PKI systems.

As starting point, any pool shall be open and accessible to all PKI participants in the EU PKI Ecosystem for e-mobility.

3.3.1 Root Certificate Pools (RCP)

1) The RCP shall provide market participants access to Root Certificates stored in the CTL.
2) The stored root certificates by the RCP shall be regularly checked with automated processes. In this respect, expired or revoked certificates shall be deleted, keeping the content of the pools fully in synch with the CTL. Concrete implementation aspects of the pools with the CTL shall be determined by EPEGMB.
3) Any PKI participants may use these pools as a mutual trust store, also having the possibility to directly check the CTL.

3.3.2 Provisioning Certificate Pools (PCP)

1) During the production of an electric vehicle, the OEM shall create a Provisioning Certificate for the vehicle. Each Provisioning Certificate shall have a unique Provisioning Certificate Identifier (PCID). The OEM shall then publish this Provisioning Certificate and its certification chain by sending it to the Provisioning Certificate Pool.

2) The PCID is the identifier for a vehicle and must match the ISO pattern PCID format as specified in ISO 15118-20. The Provisioning Certificate Pool authorises the OEM client based on this code.

3) With the publication of a Provisioning Certificate to the PCP, no information is given to the EMSP. Trusted EMSPs can only retrieve individual Provisioning Certificates if they request them through the PCID.

4) Before the storage of the Provisioning Certificate, the PCP proceeds with the following control steps:
   i. Verifies the PCIDs world manufacturer identifier (WMI) against the OEM accounts authorised WMI list.
   ii. Verifies the validity date (valid until) of each certificate from leaf to root to be in the future. (Validity shell model).
   iii. Verifies the trust chain to the OEM root certificate.

5) When an OEM needs to renew a Provisioning Certificate, they may send an updated Certificate to the PCP. The update process overwrites the existing Provisioning Certificate with the same PCID.

6) An update of a Provisioning Certificate in the pool triggers an instant push notification to all EMSPs subscribed to the corresponding PCID if the key pair changes.

7) If the Provisioning Certificate under one PCID is removed from the ecosystem, the OEM that owns it may delete it from the pool. This operation triggers the Contract Certificate Pool to delete all existing Contract Certificates linked to this Provisioning Certificate.

8) Every EMSP onboarded in the EU PKI Ecosystem is granted access to all available Provisioning Certificates in the PCP as long as they request following the market rules defined.

9) When EMSPs send the PCID of a Provisioning Certificate issued by the OEM to the PCP, they receive its Provisioning Certificate with the corresponding certificate chain.

10) No confidential OEM data, in line with applicable EU regulation (i.e., General Data Protection Regulation), can be displayed when querying the available OEM Provisioning Certificates.

11) Each PKI provider is responsible for updating and notifying each corresponding PKI participants (i.e., MOs with active contracts for the related PCID) when PCs are renewed or deleted.

12) The stored OEM Provisioning Certificates shall be regularly checked with automated processes. In this respect, expired and revoked certificates will be deleted. Deleting a provisioning certificate triggers deletion of all connected Contract Certificates from the Contract Certificate Pool.

3.3.3 Certificate Provisioning Service (CProvS)

1) The CProvS provides interfaces for generating and signing contract data of EMSP.

2) EMSPs can provide contract data to be signed by CProvS or send necessary information to CProvS to generate contract data and sign it. CProvS can return the signed contract data to the requestor and/or store it in the CCP.

3.3.4 Contract Certificate Pools (CCP)

1) The CCP stores the signed contract certificate bundles from the EMSPs and provides it for the CPOs and OEMs' back-ends.
2) The EMSPs' signed contract certificate bundle shall be stored in the CCP and assigned to their respective PCID. The CCP also enables multiple contracts storing for each PCID.
3) The CCP keeps the contracts of each EMSP separated. The defined access rules prevent unauthorised requests to other EMSPs' contracts, which means that each EMSP can only manage (create/update/delete) contracts of their own company.
4) Publishing a Contract Certificate in the pool can trigger an instant push notification to the OEM enrolled in the WMI corresponding to the contract's PCID.
5) In case an EMSP needs to renew a Contract Certificate, they shall do so, at least, by sending an updated Certificate to the CCP. The update process overwrites the existing Contract Certificate with the same EMAID and PCID. An update of a Contract Certificate in the pool can trigger an instant push notification to the OEM enrolled in the WMI corresponding to the contract's PCID.
6) If the Contract Certificate under one EMAID/PCID combination needs to be removed from the ecosystem, the EMSP that owns it shall delete it from the CCP. Deletion of a contract certificate in the CCP shall trigger an instant push notification to the OEM enrolled in the WMI corresponding to the contract's PCID.
7) The expired and revoked contract certificates shall be removed as early as possible from the Contract Certificate Pool.

3.3.5 PKI Services

1) Any PKI provider has flexibility to adapt PKI services based on market developments without impacting the core process of a PKI participant, and without disruption the governance and functioning of the EU PKI ecosystem for e-mobility.
2) Any PKI service shall provide, at least, the following information to allow for an easy comparison among them:
   i. Name and contact details of the PKI provider (operator).
   ii. Terms and conditions of PKI services.
   iii. Service elements in scope/out of scope of offer.
   iv. Service Level Agreement (SLA) information and contractual details.

3.4 Market rules for PKI Participants

The paragraphs below address the market rules for the main PKI participants, specifically EV OEMs, CPOs, and EMSPs.

To enable all parties to validate certificates from the e-mobility PKI, the PKI Participants shall provide certificate status information to all other PKI Participants without any restriction.

3.4.1 Market rules for EV OEMs

1) EV OEMs shall ensure EVs access to all V2G Root CAs in the CTL of the European PKI Ecosystem. This enables technical interoperability between both charging stations and EVs in Europe. In consequence, the same rule applies for CPOs.
2) EV OEMs shall provide non-discriminatory access to their OEM Root CAs to the PKI participants in the EU PKI Ecosystem for e-mobility ecosystem. In consequence, the same rule applies for CPOs.
3) Any EV shall be handed over to the end user without any installed contract from any given pre-selected EMSP contract, unless the consumer provides explicit agreement based on an informed choice. Without a consumer's choice, the EV is delivered without any installed contract.
4) In the delivery process, OEMs are responsible to inform the consumer about the possibility of installing a plug and charge contract of an EMSP of his/her choice.
5) Any EV OEM shall ensure non-discriminatory access and installation of contract certificates.
6) Any EV-OEM shall publish the necessary information, namely:
   i. How EMSPs can obtain the vehicle Provisioning Certificate (PC),
   ii. How EMSPs can provide Contract Certificates to be installed into the vehicle,
   iii. ISO 15118 version (-2 vs -20), schema version, cryptographical information.
7) Any EV-OEM whose vehicles support ISO 15118 (either -2 and/or -20) Plug & Charge shall allow installing, de-installing, activating, and deactivating user-preferred EMSP contract(s) in a non-discriminatory way. This includes an equal level of the technical complexity of installation and revocation processes and the display and visibility of EMSP contracts to the end user.
8) Any EV OEM shall ensure the user can obtain the PCID through the Certificate Pools as a human (string) and computer readable (QR) code from an easily accessible HMI (EV, App, etc.).
9) Any EV-OEM shall define security measures to protect against misuse of the PCID.
10) Any OEM shall ensure the PCID communicated to the user is equal to the PCID embedded in the provisioning certificate.
11) Any EV OEM shall ensure unlimited and user-friendly access to PCID for the user. Additionally, EV OEMs shall inform the user about a PCID renewal (e.g., when replacing the EVCC) in a user-friendly way.
12) Any OEM shall ensure any PCID refers to one unique EV. An EV can have multiple PCIDs.
13) Any EV OEM shall ensure there is always a valid OEM provision certificate available for the EV supporting ISO 15118 plug and charge.
14) Any EV-OEM shall deactivate and delete revoked contract certificates and inform the user in a timely manner.
15) Any EV-OEM shall not use the revocation process of certificates to potentially discriminate against EMSPs.

3.4.2 Market rules for CPOs

1) EVSE in this section means an EVSE with ISO 15118 plug and charge capability.
2) Any CPO shall ensure EVSEs access to all OEM Root CAs and EMSP Root CAs in the Trust List of the EU PKI Ecosystem for e-mobility. This enables technical interoperability between charging stations and EVs in the EU.
3) When a CPO offers contract certificate installation via EVSE then the EVSEs shall be connected to all contract certificate pools of the EU PKI Ecosystem.
4) If the Plug & Charge contract certificate installation via EVSE is not successful, the CPO shall inform the user.
5) Any CPO shall ensure that the EVSEs always have valid EVSE leaf certificates.
6) If an EVSE offers Plug & Charge and no other means of identification have been used, an EV initiates a Plug & Charge identification, then the EVSE shall start processing the Plug & Charge authentication and authorisation.
7) Any CPO is responsible for validating the Contract Certificate and its associated EMSP contract (with EMAID).
8) If the Plug & Charge identification is not being accepted by the CPO due to any reason (e.g., no certificates available, the contract can't be found, the contract is not valid, revoked), the CPO shall duly inform the end user.

3.4.3 Market rules for EMSPs

1) Any EMSP shall make available, at least, the following information to the relevant PKI participants (e.g., OEMs and CPOs):
   i. How any given CPO or EV-OEM can obtain the contract certificate (CC)?
   ii. Which ISO 15118 version (-2 vs. -20), schema version, cryptographical information is based the Contract Certificate (CC)?
2) Any EMSP shall make Contract Certificate Packages accessible to CPOs and EV-OEMs to enable the installation of contract certificates in EVs.
3) Any EMSP shall provide non-discriminatory access to their MSP Root CAs to the PKI participants in the EU PKI Ecosystem for e-mobility ecosystem.
4) Any EMSP contract certificate bundles shall be signed by a CProvS certificate chain derived from a V2G Root CA.
5) When the user ends his EMSP contract, the EMSP shall revoke all related contract certificate bundles and publish this information.

If the EV-OEM has revoked the provisioning certificate, the EMSP shall de-activate all related contract certificate bundles and add them to the revocation list.

ONBOARDING GUIDELINES

At the moment of finalising this Support Study, the onboarding guidelines are in a draft form (at disposal of the European Commission and participant members of the working group). Upon accordance with the European Commission, the revision and fine-tuning process of these guidelines was suspended to prioritise other deliverables of the Support Study. Consequently, PwC advises that the onboarding guidelines undergo a final process of

revision and further development by a group of experts selected by the European Commission.

EUROPEAN COMMISSION
Directorate-General for Mobility and Transport

Directorate B – Investment, Innovative & Sustainable Transport
B4 – Sustainable & Intelligent Transport

EUROPEAN COMMISSION SUPPORT STUDY

DEVELOPMENT OF A GOVERNANCE FRAMEWORK FOR THE EU PUBLIC KEY INFRASTRUCTURE (PKI) BASED ON THE STANDARD ISO 15118

DELIVERABLE 4 – MUTUALLY RECOGNISED SET OF CRITERIA FOR ROOT CAS, SUBSCRIBERS AND THE CTL OF THE EU PKI ECOSYSTEM FOR E-MOBILITY

Objective: The aim of this activity is **to capture the consensus between the market actors on the development of a mutually recognised set of criteria for Root CAs, Subscribers and the CTL** of the European PKI Ecosystem for e-mobility.

The activity builds on the work carried out by the participants members of the working group set up and coordinated under the European Commission Support Study.

Extension: To be discussed.

Foreword

This document is a deliverable in support of the preparation of secondary legislation (i.e., delegated and/or implementing acts) under the Alternative Fuels Infrastructure Regulation (AFIR)[36]. This concrete deliverable elaborates on the development of a governance, architecture, and implementation plan for the set-up and operation of an EU Public Key Infrastructure (PKI) ecosystem in the EU.

The document has been developed as part of the European Commission 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC. The document has also been reviewed and validated by the Sustainable Transport Forum (STF), which is established and chaired by the European Commission services since April 2015 to assist the Commission in implementing the Union's activities and programmes aimed at fostering the deployment of alternative fuels infrastructure to contribute to the European Union energy and climate goals.

The study was articulated in two phases.

Phase 1 of the 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC.

During the first phase, the study was centred around bilateral interviews with the existing PKI service providers and research projects of the Sustainable Transport Forum (STF) subgroup on Governance & Standards - namely CharIN, Gireve, Hubject, SAE, and Vedecom. The result of this phase has been the development of a set of recommendations on a high-level governance and architecture framework for the functioning and operation of a PKI ecosystem in the EU. These recommendations were later transmitted and reviewed by the STF sub-group on governance and standards, being those endorsed by the sub-group as part of the document *Activity 2 - 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*[37].

- **Recommendation 1: A regulated vs. non-regulated governance and architecture –** the STF sub-group favours a regulated approach for the governance and architecture in Europe due to the advantage of providing a clear legal basis covering key elements of the PKI.
- **Recommendation 2: Single or Multi Root CA model** - The STF sub-group members advocate for a multi-Root CA model due to the benefits of having competition in the market among several V2G Root CAs – increased variety and quality of service, reduced prices - as well as the increased operational resilience of the PKI. Also, this approach also supports the current market situation under which multiple market actors are already committed to offering the service of V2G Root CA in the EU.
- **Recommendation 3: Architecture model to ensure interoperability across Multi Root CAs** - the STF sub-group members' preferred interoperability solution across the multi-Root CA model is a Certificate Trust List (CTL), due to the solution's potential for scalability, centralised maintenance, and fitting logic of certificate verification.

[36] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1867

[37] https://op.europa.eu/en/publication-detail/-/publication/b7910659-276c-11ee-839d-01aa75ed71a1/language-en

- **Recommendation 4: Governance Model –** the STF sub-group members on G&S prefer a mixed approach, involving both private and public stakeholders. The combination of categories of entities such as businesses organisation, industry consortia and public authorities allows to leverage the strengths of each of them while minimising the downsides.
- **Recommendation 5: Ownership model** – the STF sub-group members on G&S agree on having a central public authority (i.e. European Commission) to perform the governance roles of the PKI (i.e. Definition of criteria for Root CAs operators, check of the criteria, and distribution of the CTL) while the managing and operating layer of the multiple PKI systems (i.e. operations of the PKI and the actual provision of the emission of certificates and signing service) could be covered by a combination of business organisations, industry consortia and public authorities.
- **Recommendation 6: Implementation scheme for the proposed governance and architecture solution** – the STF sub-group members on G&S agree that the development of the preferred governance and architecture solution will most likely occur in two phases. The initial phase will see the continuing of the existing Plug & Charge service solutions with their corresponding PKI implementations where the market is further tested and scaled-up by market actors. This relates in particular to existing implementations of ISO 15118-2. The second phase will be based on a regulated approach by the European Commission under a set of governance and architecture rules applicable in the EU considering the elements developed in the deliverables of this study and the recommendations of the STF Sub-group. A future PKI ecosystem will consider existing implementations based on ISO 15118-2 and, at the same time, will transition towards a future based on ISO 15118-20.

Phase 2 of the 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC.

The second phase of the study builds on the recommendations of the previous phase. Specifically, a dedicated group of experts was specifically formed to work on the following set of deliverables aiming to define the policy, technical and governance elements to guide the set-up and develop a regulated approach to a Multi-Root CA model with the CTL as the preferred interoperability solution. All this, under a mixed (public/private) governance approach:

Table 19: List of deliverables completed under the Support Study

Deliverable	Title
1	**Deliverable 1** - Architecture, governance, and operating model for a PKI based on ISO 15118;
2	**Deliverable 2** - Relevant standards and technical aspects of the PKI to allow interoperability across V2G Root CAs;
3	**Deliverable 3** - Market rules for the EU PKI ecosystem for e-mobility;
4	**Deliverable 4** - Mutually recognised set of criteria for Root CAs, Subscribers and the CTL of the EU PKI ecosystem for e-mobility;
5	**Deliverable 5** - Implementation plan for the preferred governance and

	architecture model;

More specifically, the present deliverable is the result of the work of the working group coordinated under the European Commission 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC. The organisations comprising the working group are the following members of the STF subgroup on Governance & Standards:

- CharIN,
- Gireve,
- Hubject,
- SAE,
- Vedecom,
- ChargePoint,
- ElaadNL,
- EnBW,
- Shell,
- Smartlab,
- Tesla,
- E-clearing.net.

The work developed by the working group and reflected in these deliverables has been also subject to the review and validation of the Sustainable Transport Forum (STF) Sub-group on Governance & Standards.

Scope of Deliverable 4

The **purpose of this deliverable is to outline the minimum requirements that relevant market actors (private company, public authority, etc.) shall comply with in order to be considered a trusted Root CA operator** in the EU PKI ecosystem based on ISO 15118. Specifically, these minimum requirements shall be respected by every V2G Root CA operator, and by all MOs and OEMs' Root CA operators seeking to be included in the EU PKI Ecosystem for e-mobility.

1 Requirements to be a trustworthy Root CA operator

The following requirements should apply:

- The Root CA shall be capable of generate and self-sign key pairs as needed, in accordance with the requirements of both ISO 15118-2 and ISO 15118-20. The nature of the Root CA shall determine the extent to which the compliance to ISO 15118 shall be extended.
- The Root CA, as an organisational part dealing with the PKI, shall comply with standard auditing requirements on information security carried out by accredited PKI auditors according to the requirements defined by the EPEGMB and the requirements in the CP using the ISO 27001 assessment. As a consequence, Root CA operators shall maintain a valid certification following the guidelines for an ISO 27001 audit.
- The Root CA shall have and publish a Certificate Policy (CP) based on the minimum requirements established for the EU PKI ecosystem and the RFC 3647[38] and ISO 27099[39]. In addition, the Root CA shall:
  - Define the scope of the CP including the standard definition (i.e., either ISO 15118 -2, or -20).
  - Define the territory in which the Root CA operator plans on operating, at least beyond the EU and its ecosystem, (e.g., UK, North America, etc.).
  - Define a revocation mechanism. A service working as OCSP responder must be in place.
- The V2G Root CAs must indicate in their CP that their certificates are only to be used for ISO 15118 purposes, this must also be valid for the relative Sub-CAs' certificates.
- For Root CAs and Sub-CAs' certificates the rekey is the mandated approach. Certificate rekey is the preferred approach for leaf certificates. The renewal of leaf certificate is allowed.
- Each Root CA operator shall have a OCSP responder service (either operate it directly or use an external service).

2 Requirements for subscribers of the EU PKI Ecosystem for e-mobility

The following requirements should apply:

As described in RFC 3647[40], the subscriber for the certification services of a particular CA is the person or organisation that has a contract with that CA and is authorised to request the CA to sign certificates. In the context of PKI systems for e-mobility, subscribers are organizational entities. Thus:

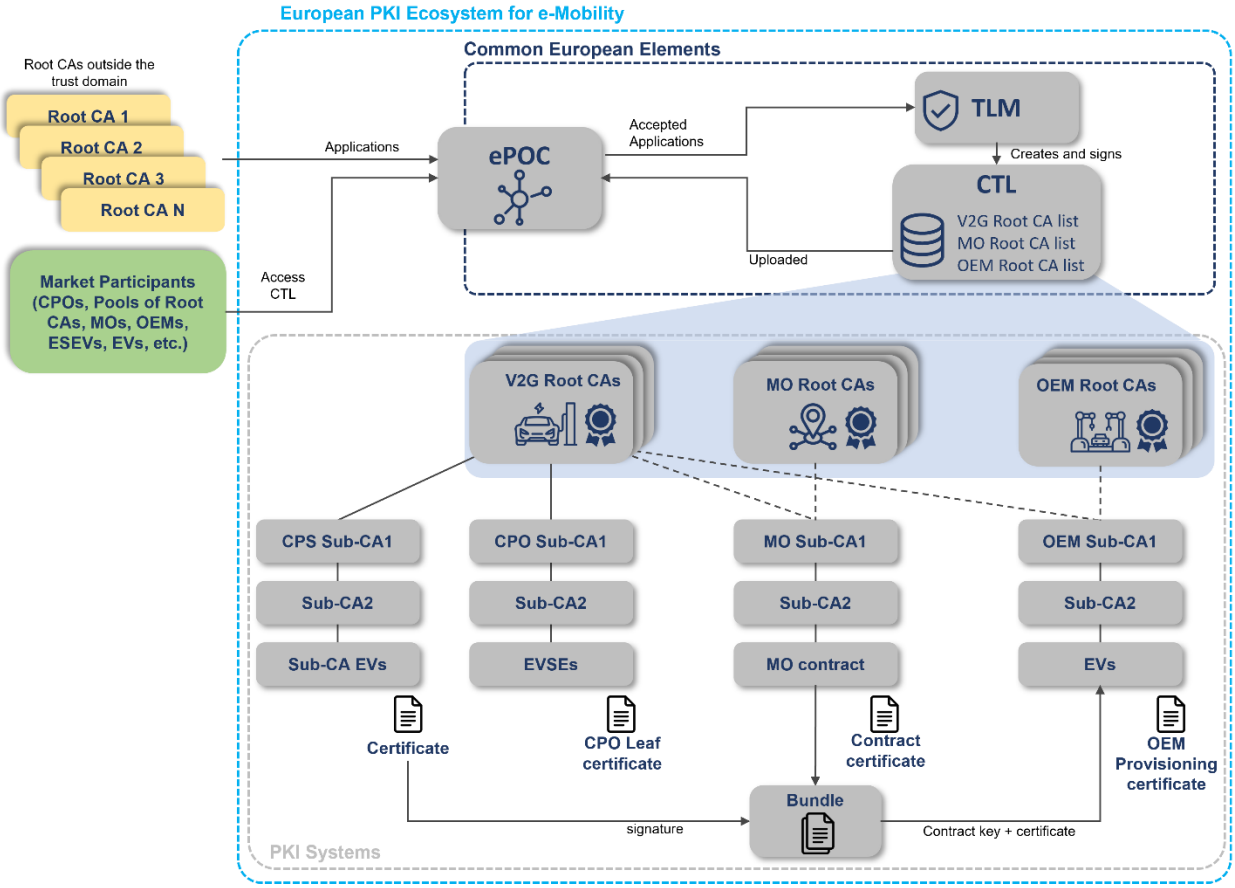
---

[38] https://www.rfc-editor.org/info/rfc3647
[39] https://www.iso.org/standard/56590.html

[40] RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (2003). Available at: https://www.rfc-editor.org/info/rfc3647

- The subscribers for the Root CA are the Sub-CA1 of the CPO, CPS, MO and OEM. The Sub-CA1 can be used only in relation to one branch.
- The subscribers for a Sub-CA1 are the Sub-CA2s in the respective branch.
- The subscribers for a CPO Sub-CA2 are Charge Point operators.
- The subscribers for a CPS Sub-CA2 are Certificate Provisioning Services. As described in ISO 15118-2 and -20, this role may be fulfilled by a Mobility Operator, a SECC operator, or a dedicated CPS operator.
- The subscribers for a MO Sub-CA2 are Mobility Operators.
- The subscribers for an OEM Prov Sub-CA2 are OEMs of electric vehicles.

Figure 23: Architecture model for the EU PKI ecosystem for e-mobility



The Root CA shall integrate and expand the following responsibilities for subscribers in their respective CP. The subscribers shall be responsible for:

- Indicating registered contact points and authorized administrators.
- Timely sending certificate applications to the respective RA.
- Ensuring the accuracy of the information in any certificate application sent.
- Accepting or rejecting any issued certificate.
- Using any certificate according to all applicable requirements.
- Notifying the respective CA without delay in case:
  - The data in the certificate is, or becomes, inaccurate.

- A compromise of the private key associated with a certificate is proven or suspected.
- The subscriber has lost control over the private key associated with a certificate. In case the private key is located in an EVCC or SECC, this includes cases of theft, malfunctioning, or destruction.

3 Requirements for the EU CTL

- The EU PKI ecosystem for e-mobility and its single CTL will only include those valid and accepted Root Certificates.
- The most updated version of the CTL shall be retrieved by the interested market parties consulting the ePOC. It is advised that this operation should be done, at least, once per day and at the minimum shall be performed once per week.
- The CTL relevant content shall be transferred in the EVs and EVSEs through the Root Certificate Pool system.

EUROPEAN COMMISSION
Directorate-General for Mobility and Transport

Directorate B – Investment, Innovative & Sustainable Transport
B4 – Sustainable & Intelligent Transport

EUROPEAN COMMISSION SUPPORT STUDY

DEVELOPMENT OF A GOVERNANCE FRAMEWORK FOR THE EU PUBLIC KEY INFRASTRUCTURE (PKI) BASED ON THE STANDARD ISO 15118

DELIVERABLE 5 – IMPLEMENTATION PLAN FOR THE PREFERRED GOVERNANCE AND ARCHITECTURE MODEL

Objective: The aim of this activity is to define the **governance, architecture, and operating model** for a PKI based on ISO 15118, in line with recommendation of phase 1 of the Support study on the development of a governance framework for the Public Key Infrastructure (PKI) based on the standard ISO 15118.

The activity builds on the work carried out by the participant members of the working group set up and coordinated under the European Commission Support Study.

Extension: To be discussed.

Foreword

This document is a deliverable in support of the preparation of secondary legislation (i.e., delegated and/or implementing acts) under the Alternative Fuels Infrastructure Regulation (AFIR)[41]. This concrete deliverable elaborates on the development of a governance, architecture, and implementation plan for the set-up and operation of an EU Public Key Infrastructure (PKI) ecosystem in the EU.

The document has been developed as part of the European Commission 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC. The document has also been reviewed and validated by the Sustainable Transport Forum (STF), which is established and chaired by the European Commission services since April 2015 to assist the Commission in implementing the Union's activities and programmes aimed at fostering the deployment of alternative fuels infrastructure to contribute to the European Union energy and climate goals.

The study was articulated in two phases.

Phase 1 of the 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC.

During the first phase, the study was centred around bilateral interviews with the existing PKI service providers and research projects of the Sustainable Transport Forum (STF) subgroup on Governance & Standards - namely CharIN, Gireve, Hubject, SAE, and Vedecom. The result of this phase has been the development of a set of recommendations on a high-level governance and architecture framework for the functioning and operation of a PKI ecosystem in the EU. These recommendations were later transmitted and reviewed by the STF sub-group on governance and standards, being those endorsed by the sub-group as part of the document *Activity 2 - 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*[42].

- **Recommendation 1: A regulated vs. non-regulated governance and architecture –** the STF sub-group favours a regulated approach for the governance and architecture in Europe due to the advantage of providing a clear legal basis covering key elements of the PKI.
- **Recommendation 2: Single or Multi Root CA model** - The STF sub-group members advocate for a multi-Root CA model due to the benefits of having competition in the market among several V2G Root CAs – increased variety and quality of service, reduced prices - as well as the increased operational resilience of the PKI. Also, this approach also supports the current market situation under which multiple market actors are already committed to offering the service of V2G Root CA in the EU.
- **Recommendation 3: Architecture model to ensure interoperability across Multi Root CAs** - the STF sub-group members' preferred interoperability solution across the multi-Root CA model is a Certificate Trust List (CTL), due to the solution's potential for scalability, centralised maintenance, and fitting logic of certificate verification.

[41] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1867
[42] https://op.europa.eu/en/publication-detail/-/publication/b7910659-276c-11ee-839d-01aa75ed71a1/language-en

- **Recommendation 4: Governance Model –** the STF sub-group members on G&S prefer a mixed approach, involving both private and public stakeholders. The combination of categories of entities such as businesses organisation, industry consortia and public authorities allows to leverage the strengths of each of them while minimising the downsides.
- **Recommendation 5: Ownership model** – the STF sub-group members on G&S agree on having a central public authority (i.e. European Commission) to perform the governance roles of the PKI (i.e. Definition of criteria for Root CAs operators, check of the criteria, and distribution of the CTL) while the managing and operating layer of the multiple PKI systems (i.e. operations of the PKI and the actual provision of the emission of certificates and signing service) could be covered by a combination of business organisations, industry consortia and public authorities.
- **Recommendation 6: Implementation scheme for the proposed governance and architecture solution** – the STF sub-group members on G&S agree that the development of the preferred governance and architecture solution will most likely occur in two phases. The initial phase will see the continuing of the existing Plug & Charge service solutions with their corresponding PKI implementations where the market is further tested and scaled-up by market actors. This relates in particular to existing implementations of ISO 15118-2. The second phase will be based on a regulated approach by the European Commission under a set of governance and architecture rules applicable in the EU considering the elements developed in the deliverables of this study and the recommendations of the STF Sub-group. A future PKI ecosystem will consider existing implementations based on ISO 15118-2 and, at the same time, will transition towards a future based on ISO 15118-20.

Phase 2 of the 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC.

The second phase of the study builds on the recommendations of the previous phase. Specifically, a dedicated group of experts was specifically formed to work on the following set of deliverables aiming to define the policy, technical and governance elements to guide the set-up and develop a regulated approach to a Multi-Root CA model with the CTL as the preferred interoperability solution. All this, under a mixed (public/private) governance approach:

Table 20: List of deliverables completed under the Support Study

Deliverable	Title
1	**Deliverable 1** - Architecture, governance, and operating model for a PKI based on ISO 15118;
2	**Deliverable 2** - Relevant standards and technical aspects of the PKI to allow interoperability across V2G Root CAs;
3	**Deliverable 3** - Market rules for the EU PKI ecosystem for e-mobility;
4	**Deliverable 4** - Mutually recognised set of criteria for Root CAs, Subscribers and the CTL of the EU PKI ecosystem for e-mobility;
5	**Deliverable 5** - Implementation plan for the preferred governance and architecture model;

More specifically, the present deliverable is the result of the work of the working group coordinated under the European Commission 'Support study on the development of a governance framework for the Public Key Infrastructure (PKI) under the standard ISO 15118' by PwC. The organisations comprising the working group are the following members of the STF subgroup on Governance & Standards:

- CharIN,
- Gireve,
- Hubject,
- SAE,
- Vedecom,
- ChargePoint,
- ElaadNL,
- EnBW,
- Shell,
- Smartlab,
- Tesla,
- E-clearing.net.

The work developed by the working group and reflected in these deliverables has been also subject to the review and validation of the Sustainable Transport Forum (STF) Sub-group on Governance & Standards.

Scope of Deliverable 5

The **purpose of this deliverable is to reflect the proposed way forward by the European Commission in order to support the development of a EU PKI ecosystem for e-mobility**. In concrete terms, this deliverable describes the concrete action in order to set-up and implement the high-level governance and architecture framework elaborated in this study and considering the recommendations by the STF Sub-group on Standards (Activity 2). In that manner, this document gathers the concrete steps in terms of legislative process (AFIR delegated/implementing acts), governance bodies set-up and PKI technical implementation and operation to put in place a EU PKI ecosystem for e-mobility based on a regulated framework to a Multi-Root CA model with the CTL as the interoperability solution.

Finally, it is important to note that this deliverable presents a proposed approach to the European Commission as part of the study. Therefore, it is ultimately a decision from the European Commission to endorse and carry out the roadmap elaborated in this deliverable.

1 Roadmap for the set-up and implementation of the EU PKI Ecosystem for e-mobility

The regulatory set-up and technical implementation of the governance and architecture framework of the EU PKI ecosystem for e-mobility, as defined in Deliverable 1, will take place after official announcement by the European Commission (EC) on 2 June 2023 during the STF Plenary to lead the developments for the establishment of a EU PKI ecosystem for e-mobility, with the concrete technical set-up of a CTL as of January 2025.

It is important to note that this document, as part of the overall Support Study, is supporting the EC on their decision making. However, the EC might well decide to carry out some modifications to the concrete elements elaborated in the Support Study depending on a number of factors, such as the technical readiness of the deliverables required for the implementation, the internal budget and human resources available or the market readiness to support this project.

In any event, as outlined in Phase 1 of the Support Study, the roadmap leading to a full and consolidated implementation of a EU PKI ecosystem for e-mobility would be split into two clear phases. First, an initial market driven implementation based on the existing solutions that market actors are testing and progressively starting to offer to their customers. During this initial phase there would not be EU wide interoperability, neither a regulated approach with common rules and procedures. Second, a EU PKI ecosystem would be set-up following a unique interoperability solution subject to the concrete regulatory requirements established by the EC under AFIR secondary legislation. The EC decision on this matter and subsequent regulatory action will help coordinating market actors in the EU towards a unique interoperability solution with common rules and requirements, scaling it up to be able to accommodate for the expected growth of e-mobility.

This document gathers as a result of this study and consultation with market actors a roadmap that leads to a full and consolidated implementation of a EU PKI ecosystem for e-mobility. For that, this roadmap presents the main procedural steps to achieve that. In consequence, it associates concrete action to both the relevant governance (e.g., set up of the governance bodies, etc.) and technical elements (e.g., definition of technical specifications for interoperability of CTL with ISO 15118) required to set-up the EU PKI ecosystem in line with Deliverable 1.

Finally, this roadmap represents a *de facto* agreement by participant industry members to support the work elaborated under this study with this accompanying roadmap.

2 Main steps for the establishment of a EU PKI Ecosystem for e-mobility

To take into practice the required elements for the set-up and implementation of a EU PKI ecosystem with a common governance and architecture framework the following action points must be carry out:

1) Decision by the EC on the proposed approach to the governance and architecture interoperability of the EU PKI ecosystem for e-mobility.
2) Adoption by the EC of the relevant delegated and implementing acts in support of the EU PKI ecosystem for e-mobility.
3) Set-up by the EC of the relevant bodies (expert groups) for the management and operation of the EU PKI ecosystem.

4) Development by European/International Standardisation Organisations and market actors of the CTL technical specification and relevant protocols for the functioning of the EU PKI ecosystem.
5) Full implementation.

3 Decision by the EC on the proposed approach to the governance and architecture interoperability of the EU PKI Ecosystem for e-mobility

Following the finalisation of this Support Study and considering the work performed and the STF Sub-group on Governance & Standards, the EC was expected to announce the proposed way forward in relation to the future EU PKI ecosystem for e-mobility. **On 2 June 2023, the EC announced during the STF Plenary its intention to set-up a EU PKI CTL as part of a new EU-wide ecosystem for e-mobility**. As part of this announcement, **the EC indicated the consideration of all the elements reflected in the STF and during this Support Study to put in place this new ecosystem, from a regulatory perspective but also from a governance, technical and resource perspective**.

The full deployment of the EC preferred governance and architecture would take some time. However, the set-up of the ecosystem is conceived to start at the moment the EC announces the way forward. In practice, market actors will continue developing and bringing to the market their Plug & Charge solutions with the use of ISO 15118-2. This will start already configurating the architecture of a Multi-Root CA model where different PKI systems will operate and offer services within the EU PKI ecosystem. During that period of time, the EC with their proposed approach will adopt the relevant delegated/implementing acts under AFIR that will set-up the legal basis for the EU PKI ecosystem. That regulatory approach is expected to establish the minimum requirements that all participants PKI system operators and market actors in the EU shall comply with. The application of that regulatory approach occurs typically between 12 and 24 months after the adoption by the EC, thus, it provides the necessary transition period for the market to adjust.

After this first phase of transition, once the EC has adopted the delegated/implementing acts that underpin the EU PKI ecosystem a second phase will start. In this second phase, both the EC and market actors will work together to set-up the proposed governance and architecture framework. Moreover, from that moment on, the concrete requirements established in the delegated/implementing acts will guide further the process.

4 Adoption by the EC of the relevant delegated and implementing acts in support of the EU PKI ecosystem for e-mobility

After the announcement by the EC on the approach for the EU PKI ecosystem for e-mobility, preparation works will start that will lead to the adoption of relevant delegated/implementing acts under AFIR to regulate this matter.

As emerged from the first phase of the support study, the preferred governance and architecture for interoperability of the EU PKI ecosystem for e-mobility is the CTL approach integrating PKI systems based on ISO 15118. Importantly, it has been developed a common understanding with participant market actors by which it is accepted that the EU PKI ecosystem will use both ISO 15118-2, as its initial implementation solution, in a process that

will lead towards a full transition to ISO 15118-20, which includes enhanced capabilities. Thus, both ISO 15118-2 and -20 will be part of the EU PKI ecosystem with the goal of migrating progressively towards -20.

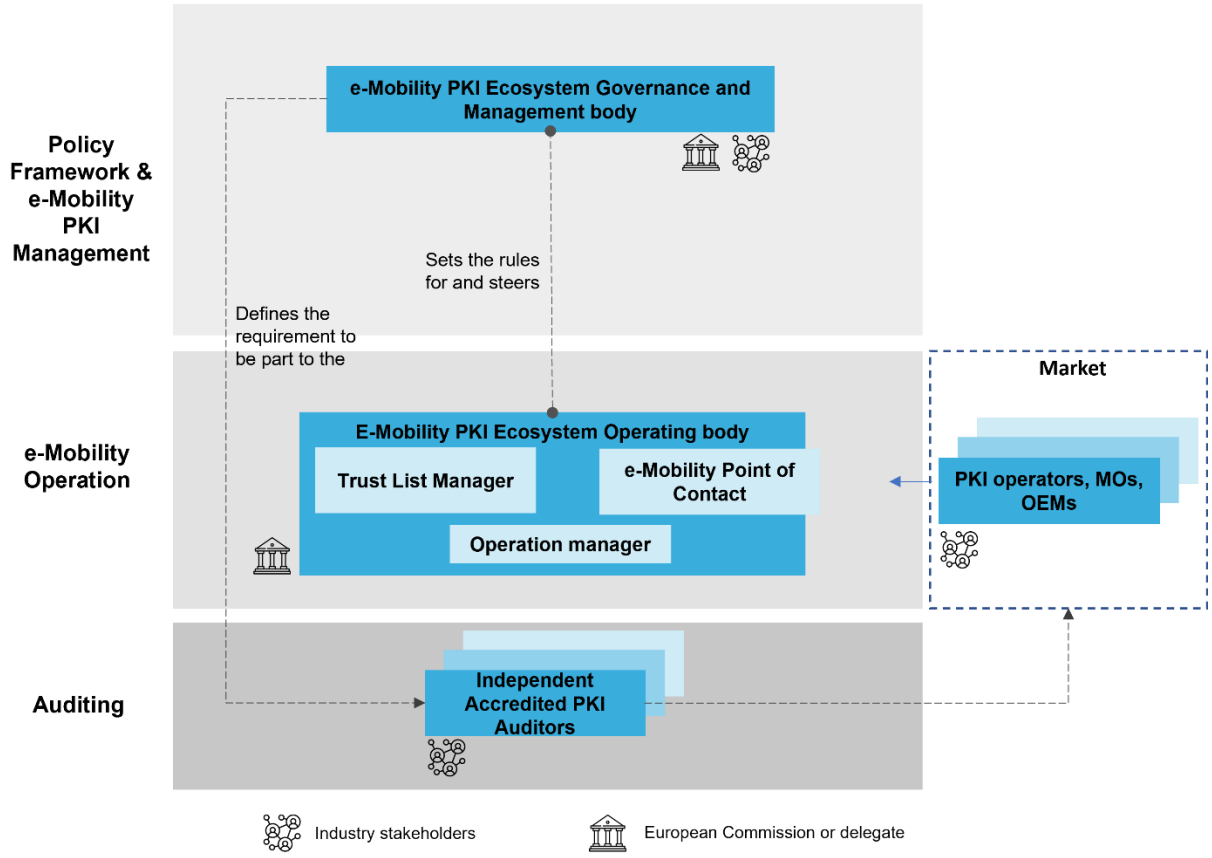
The upcoming EC's delegated and implementing acts are to provide legal clarity on this matter. Consequently, it is expected that the following acts will address the following aspects:

- Commission Delegated Regulation (CDR): it will prescribe key concrete standards (ISO 15118-2 and/or -20) in support of the EU PKI ecosystem building on the are identified in AFIR Annex II on technical specifications.
- Commission Implementing Regulation (CIR): it will legally define and prescribe the relevant elements of the EU PKI ecosystem for e-mobility. The CIR would consist in a series of minimum legal requirements for participant market operators of the EU PKI ecosystem offering Plug & Charge services. Any market actor (i.e., including foreign consortia) aiming to offer Plug & Charge services in the EU will have to comply with these rules. In order to provide clarity on the implementation, as well as a constructive and smooth implementation of the CTL interoperability approach including interoperability with other future PKI ecosystems, the CIR will establish the relevant bodies (i.e., expert groups) that will be in charge of the governance, management and operations of the EU PKI ecosystem. Finally, the CIR and subsequent updates to its first adoption will include and prescribe the relevant technical specifications for the CTL (see point 2.4).

It is important to note that the future EU PKI ecosystem for e-mobility would not be limited to Plug & Charge, for which the CIR on the EU PKI ecosystem would reflect that possibility to increase in scope. To this respect, other use cases and applications will be analysed and considered by the bodies (expert groups) of the EU PKI ecosystem in communication with the EC.

With regards to the concrete bodies (i.e., expert groups) in charge of the governance, management and operation of the EU PKI ecosystem and their corresponding roles and responsibilities, please check those in Deliverable 1. A summary is presented in the figure below. These bodies are to be specifically defined in the CIR with a clear assignation of roles and responsibilities.

Figure 24: Governance model for the EU PKI ecosystem for e-mobility



5 Set-up by the EC of the relevant bodies (expert groups) for the governance management and operation of the EU PKI ecosystem for e-mobility

Once the CID and CIR are adopted, the EC would proceed to set-up the relevant bodies for the governance, management and operation of the EU PKI ecosystem. To this respect, as conveyed in the graph above (Fig. 1) and detailed in Deliverable 1, the following bodies would be established following the corresponding legal definition in the CIR:

- **E-mobility PKI Ecosystem Governance and Management body**: It would be composed by a group of experts from the EC, Member States, and a heterogeneous representation of stakeholders from the industry with interest in the offering of Plug & Charge services in the EU (i.e., PKI project providers, equipment manufacturers, vehicle manufacturers, etc.). The participation in the expert group would be defined typically through the launch of a call for applications by the European Commission. This body could well take the form of a new dedicated expert sub-group under the STF. The body will count with its corresponding Terms of Reference (ToR) and Rules of Procedure (RoP). As core function, it will be responsible to establish a general strategy applicable to the EU PKI ecosystem in line with potential regulatory aspects defined in the EU for the management and operation of a EU PKI ecosystem. It will deal also with technical aspects[43].

[43] All relevant roles and responsibilities are defined in Deliverable 1

- **E-mobility PKI Ecosystem Operating body**: This role would be covered by the EC and/or a delegate such as the JRC. The Commission may request the aid of external contractors selected via a tendering process in support of these activities (notably the procurement of ICT systems implementing the functions under the operational responsibility of the Commission). In that case, the EC would ensure the lack of conflict of interest between organizations offering Plug & Charge services and organizations that would support the operation of the operating body and the CTL. Procedurally, the Operating Body would be composed by the Trust List Manager (TLM), the e-Mobility Point of Contact (ePOC), and the Operations Manager (OM).

In addition to the bodies described in this section, for a well-functioning, secure and trustable e-mobility ecosystem a set of independent accredited PKI Auditors is needed to perform the auditing of Root CA operators (V2G, OEMs, and MOs). The PKI accredited auditor must be external and independent from the audited PKI system. Each PKI system will be to choose its PKI auditor in the market. As key factor, to ensure a level play field with EU-wide acceptance of the auditing performed, the PKI auditor will have to be chosen from of recognised members of European Accreditation[44].

Finally, it is also important to remark that until the constitution of the *E-mobility PKI Ecosystem Governance and Management body*, which will take over the EU PKI ecosystem work, the STF Sub-group on Governance & Standards will continue to be the main EC expert groups for this matter. In the future, the STF Sub-group on Governance & Standards will continue to exist with a defined vision of topics to address in relation to many other standardisations and data matters working together with the STF Sub-group on Data.

6 Development by European/International Standardisation Organisations and market actors of the CTL technical specifications and relevant protocols for the functioning of the EU PKI Ecosystem for e-mobility.

A fundamental aspect for the success of the EU PKI ecosystem and its scale-up is the adoption of relevant technical specifications that shore up its functioning. To address this point in a comprehensive manner, Deliverable 2 as part of this support study carried out a gap analysis of the different communication strands with a focus on ensuring communication and interoperability of the EU PKI ecosystem based on a CTL interoperability approach with a hybrid governance model (public/private).

As a result of this analysis, it can be concluded that to ensure full interoperability of the future EU PKI ecosystem a significant number of high-level uses cases need to be covered between a series of actors (OEMs, EVs, PCPs, CPOs, EMPSs, and the CTL). These include mainly:

- Availability of provisioning certificates to EMSPs.
- Collection of V2G Root CAs certificates to be installed in the EVs.

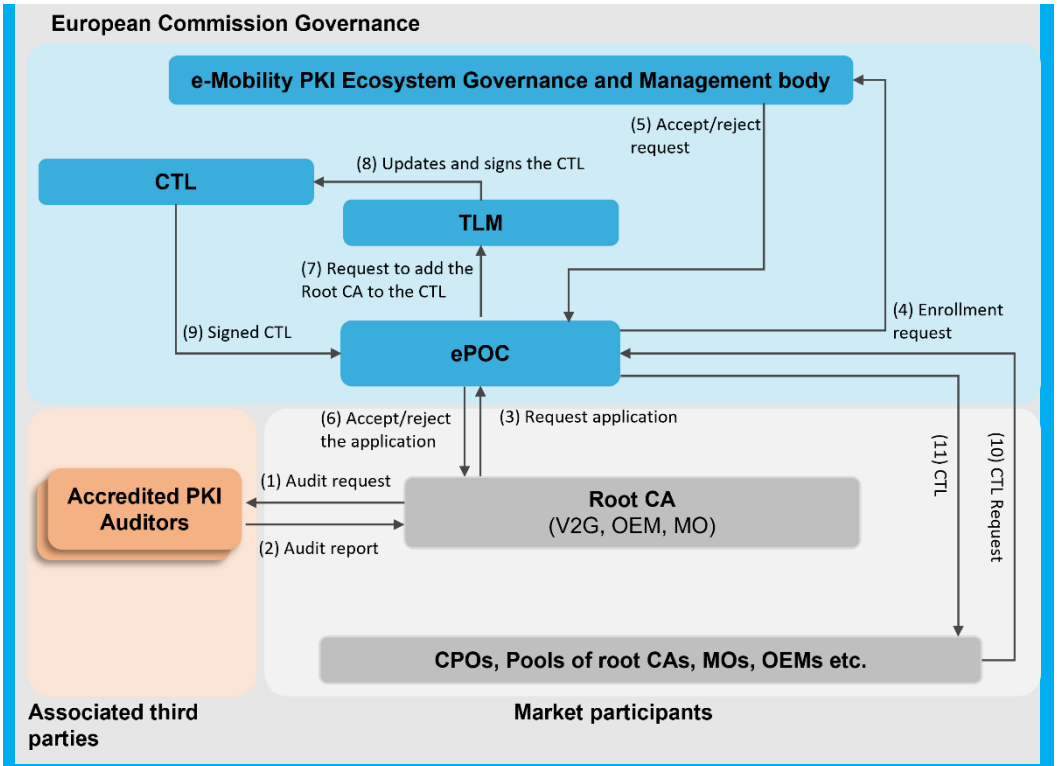
[44] https://european-accreditation.org

- Request of provisioning certificates (PCs) with (PCIDs) to enable the creation of contract certificates (CCs).
- Access of the CTL to check OEM root and verification of provisioning certificate.
- Root certificate pool access to the CTL from the ePOC.
- Availability of available certificates in the OEMs and/or CPOs pools.
- Provisioning of contract certificates (CCs) in the EVs.
- EVs sending of installation request via PCIDs.
- Retrieval by CPO of contract certificates (CCs) to be installed in the EV via the charging infrastructure.
- EVs information to OEM on the contract certificates (CCs) status.
- OEMs information to pools on the contract certificates (CCs) installation and revocation.
- EVs information to pools on the contract certificates (CCs) installation and revocation.
- CPOs information to pools on the contract certificates (CCs) installation and revocation.
- Contract certificate pools information to pools on the contract certificates (CCs) installation and revocation.
- Transfer of CC of any PKI to the charging point and the CPO.
- Collection of the MO Root CAs to be used for Contract Certificate validation.
- Request of CPO authorisation from CPO via e-roaming.

In addition, a series of additional aspects linked exclusively to the CTL would need to be standardised, such as the EU PKI ecosystem ePOC protocol[45]. These protocols would cover the **inward and outward communication flows from the ePOC** to the TLM, the CTL, the Root CAs and the market parties that would need to have access to the CTL. More specifically, it would cover the information flows 3, 4, 5, 6, 7, 9, 10, 11 represented in the image below (grey rows in the table).

[45] As a reference the one for C-ITS: https://op.europa.eu/en/publication-detail/-/publication/85151cc1-2444-11e9-8d04-01aa75ed71a1

Figure 25: Operating model for the EU PKI ecosystem for e/mobility and link with technical specifications



#	Sender	Receiver	Action
1	Root CA	Accredited PKI Auditor	Audit request
2	Accredited PKI Auditor	Root CA	Audit report
3	Root CA	ePOC	Request application to be included in the CTL
4	ePOC	ePEGMB	Enrolment request for the Root CA that submitted a valid application
5	ePEGMB	ePOC	Accept/reject the enrolment request
6	ePOC	Root CA	Information about the acceptation of rejection of the application
7	ePOC	TLM	Request to add the Root CA certificate information to the CTL
8	TLM	CTL	Update and sign the CTL with the new information
9	CTL	ePOC	The signed CTL is transmitted to the ePOC
10	Market participants	ePOC	Request of the updated CTL

11	ePOC	Market participants	CTL

Of particular importance is the definition of the:

- official application process and form for the application of Root CAs to the ePOC to be integrated in the CTL (3);
- administrative process of the ePOC;
- publishing and distributing rules of the CTL (10, 11).

To carry out this work in a consistent manner, and avoid a situation of market fragmentation with different overlapping actions, the EC aims to reach a common approach for standardisation with market actors.

6.1 Current context

During the elaboration of this study, it was communicated by participants members the ongoing work on the so-called **Open Plug and Charge Protocol (OPNC) project**. The goal of this project would be to specify an open-source interface for Plug and Charge environments based on ISO 15118. The project was initiated by Hubject with CharIn taking over the governance of the group with the intention of scaling-up its development and having a neutral organization, where all interested organizations could work together.CharIN has set-up a dedicated OPNC task force, and it is expected that the first version of the protocol will be ready by the end of the year.

On the other side, there exists also discussions ongoing to potentially develop these technical specifications as part of other industry de facto protocols such as the Open Charge Point Interface protocol (OCPI). At the moment of elaborating this deliverable, there was not clear industry consensus on how to proceed.

It is **a key concern as part of this Support Study and for the EC the materialisation of a situation where a number of actors would take different positions and start working on separate overlapping projects with the intention to bring as soon as possible to the market the same sort of solutions**. It is however **the role of the EC in view of harmonisation the future governance and architecture of the EU PKI ecosystem that different standardisation actions are aligned and contribute to the same goal**. Importantly, the relevant technical specifications (and their protocols and standards) shall be part of the future CIR and potential updates laying down the governance of the EU PKI ecosystem. For this reason, it is gathered in this section an agreed way forward.

6.2 Work approach to address existing gaps

Considering the above-mentioned situation, the European Commission as part of the Support Study reached an agreement with CharIN OPNC taskforce to proceed in the following manner to address the standardisation gap of the EU PKI CTL:

- Development of technical specifications for OPNC by CharIN platform with participation of al potentially interested industry members. Peer-review and validation of results achieved with the STF Sub-group on Governance & Standards / EC.
- Convergence of potential comments at technical level of OPNC, and further validation / full endorsement by the STF.
- Potential endorsement of these technical specifications by the CIR in support of the EU PKI ecosystem, if meeting the requirements and compatibility with the EU PKI CTL.
- Delivery of technical specifications to an International/European Standardisation Organisations, such as IEC, ISO, ETSI, CEN-CENELEC, etc.
- In terms of timing, CharIN taskforce is expected to have ready a first version of OPNC by the end of 2023. As of September 2023, the EC with the Sub-group on Governance &

Standards will monitor the developments and ensure technical compatibility with the specifications for the CTL.

6.3 Full implementation

The full implementation will be achieved when the EU PKI ecosystem is exclusively run by the e-mobility PKI Ecosystem Governance and Management body and the e-mobility Operations body under a CTL interoperability approach for the participant PKI system, all with a hybrid governance model (public/private). At that moment, Plug & Charge solutions would be applied in ISO 15118-2 with implementations clearly transitioning to ISO 15118-20. Likewise, all market solutions would be subject to the requirements and rules established at EU level by secondary legislation under AFIR.

Finally, it is considered essential for this full implementation that technical specifications on key standards such as ISO 15118 are also endorsed by EU legislation under type approval to ensure an intertwined mandate between infrastructure and OEMs.

7 Timeline for the implementation of a EU PKI Ecosystem for e-mobility

This final section aims to present the potential timeline of the implementation roadmap for the preferred governance and architecture for the European PKI for e-mobility. This deliverable presents a proposed approach to the EC as part of this study. Therefore, it is ultimately a decision from the EC to endorse and carry out the roadmap with the time indicated here. The EC has already announced its intention to move forward with the set-up of the technical implementation for the CTL as of January 2025

Proposed approach and indicative timeline

Relevant secondary legislation under AFIR with a direct implication on the EU PKI ecosystem:

1) **Commission Delegated Regulation** (standards under AFIR Annex II) – **Q4 2023 /Q1 2024**
2) **Commission Implementing Regulation** (Public Key Infrastructure for electromobility governance & architecture) – **Q4 2023 /Q1 2024**

Other relevant secondary legislation under AFIR with an indirect but reinforcing implication on the EU PKI ecosystem in terms of data exchanges:

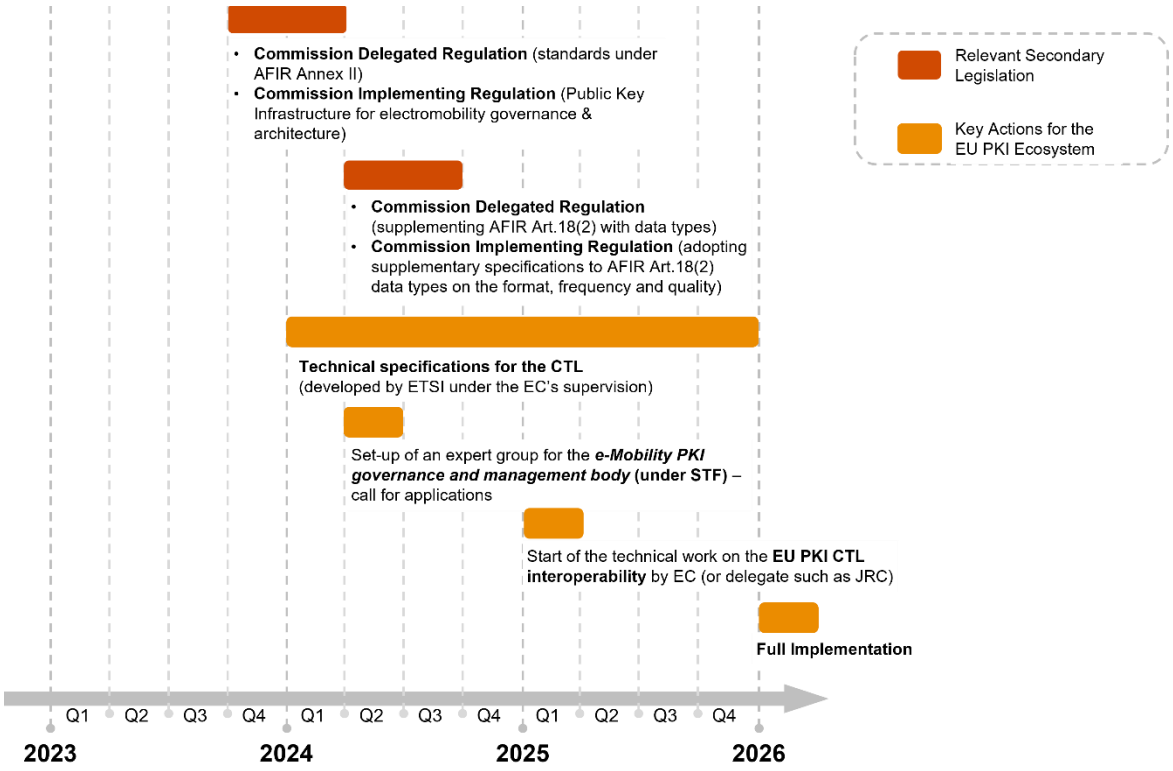
3) **Commission Delegated Regulation** (supplementing AFIR Art.18(2) with data types) – **Q2/Q3 2024**
4) **Commission Implementing Regulation** (adopting supplementary specifications to AFIR Art.18(2) data types on the format, frequency and quality) – **Q2/Q3 2024**

Preparation of related processes in parallel for simplification of procedures: CDR and CIM on standards and Public Key Infrastructure (1+2). CDR and CIM on data (3+4)

Proposed indicative timeline for key action on the EU PKI ecosystem

- Set-up of an expert group for the ***e-mobility PKI governance and management body*** **(under STF)** – call for applications – Q2 2024
- Start of the technical work on the **EU PKI CTL interoperability** by EC (or delegate such as JRC) – Q1 2025
- Full implementation – Q1 2026
- Technical specifications for the CTL to be developed by ETSI under coordination of the European Commission, using technical work from C-ITS – Q4 2024.

Figure 26: Implementation roadmap for the preferred governance and architecture for the EU PKI ecosystem for e-mobility



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-02-23-118-EN-N

Publications Office
of the European Union

doi: 10.2832/803672
ISBN 978-92-68-08397-0