mobena

Next generation EV charging

Webinar

Plug & Charge

September 24th, 2024

Understanding and Implementing Plug & Charge for eMSPs, CPOs and OEMs

INSTITUT VEDECOM

R&D INSTITUTE, FUTURE MOBILITIES TOWARDS ENERGY TRANSITION.

SPEAKERS

Gilles Chèné
Business Development Director at Thales

Jean-Marc Rives
CTO at Gireve

Steffen Rhinow
Director of P&C and Solutions at Hubject

Phanuel Hieber
Product Manager at Vector

MODERATOR

Ahmed Amine Melhaoui
Project Manager at Vedecom

About MOBENA

The project at a glance

- **MOBENA** is **the cross-sectoral** convergence point**,** acting as a **catalyst for smart energy management for EV charging,** while ensuring **symbiosis** between **ecosystems**

- **The consortium** brings together **key players in the electric vehicle charging ecosystem in France** and progressively across **Europe :**

- The consortium **coordinates** the electric vehicle charging ecosystem to ensure a harmonized deployment of Plug & Charge and **Smart Charging** functionalities.

- **Key sectors : Electromobility, Infrastructure & building, and energy sector.**

About MOBENA

Project Stakeholders

Coordinator

INSTITUT VEDECOM

OPERATIONAL PARTNERS (Steering Committee)

Electric Vehicle Manufacturers

STELLANTIS
RENAULT

Charging operators & mobility service providers

TotalEnergies
WattzHub
freshmile
VINCI ENERGIES

Charging Station Manufacturers

hager
legrand
Schneider Electric

Ecosystem providers (roaming, PKI, pools)

eTAS
HUBJECT
Gireve

Test equipments suppliers

VECTOR
Transpolis

Technology suppliers

THALES

INSTITUTIONAL PARTNERS (Initiative Committee)

E-Mobility

Avere FRANCE
PFA FILIÈRE AUTOMOBILE & MOBILITÉS
CSIAM CHAMBRE SYNDICALE INTERNATIONALE DE L'AUTOMOBILE ET DU MOTOCYCLE

Infrastructure & buildings

GIMELEC Nous décuplons les énergies
Sigeif SERVICE PUBLIC DU GAZ, DE L'ÉLECTRICITÉ ET DES ÉNERGIES LOCALES EN ÎLE-DE-FRANCE

Energy

think SMARTGRIDS
UFE Union Française de l'Electricité
MEDEE Maîtrise Energétique des Entraînements Electriques

AGENDA :

1 **Understanding Plug & Charge**

2 Ensuring Interoperability

3 Implementation Requirements

4 The future of Plug & Charge

- **If you have any questions, please, put them on the chat or the Q/R list**
- **Don’t hesitate to raise hand if you have questions**
- **The webinar will be recorded**

mobena

Next generation EV charging

What the service is ?

VISIT MOBENA.ORG FOR MORE INFORMATION

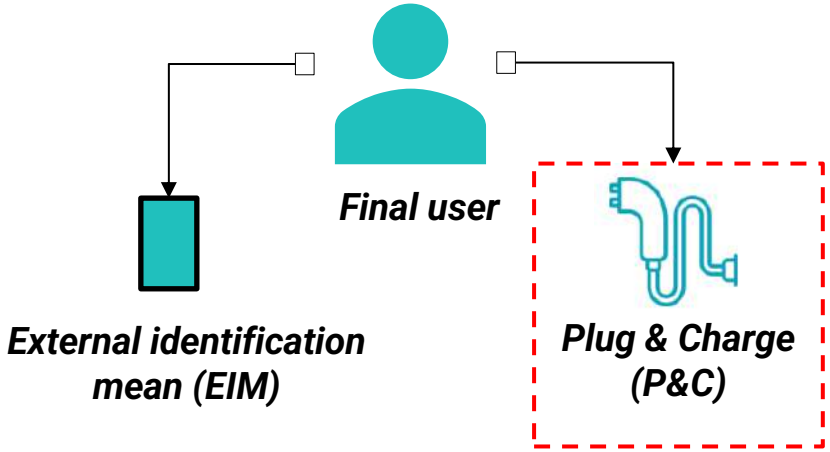
INSTITUT VEDECOM

Understanding Plug & Charge

What the service is ?

- **Plug & Charge,** in brief, is **an alternative solution** for using **multiple badges** to charge electric vehicles.
  "You plug in the cable.. and the charging process starts automatically" :

  - The terminal recognizes the contract certificate that is embedded in the vehicle, validates and proceeds charging
  - It automatically identifies the EV user's service contract by simply connecting the charging cable between the vehicle and the terminal (How ?)
  - A solution defined and framed in ISO 15118 standard



mobena

Next generation EV charging

Why the service is valuable ?

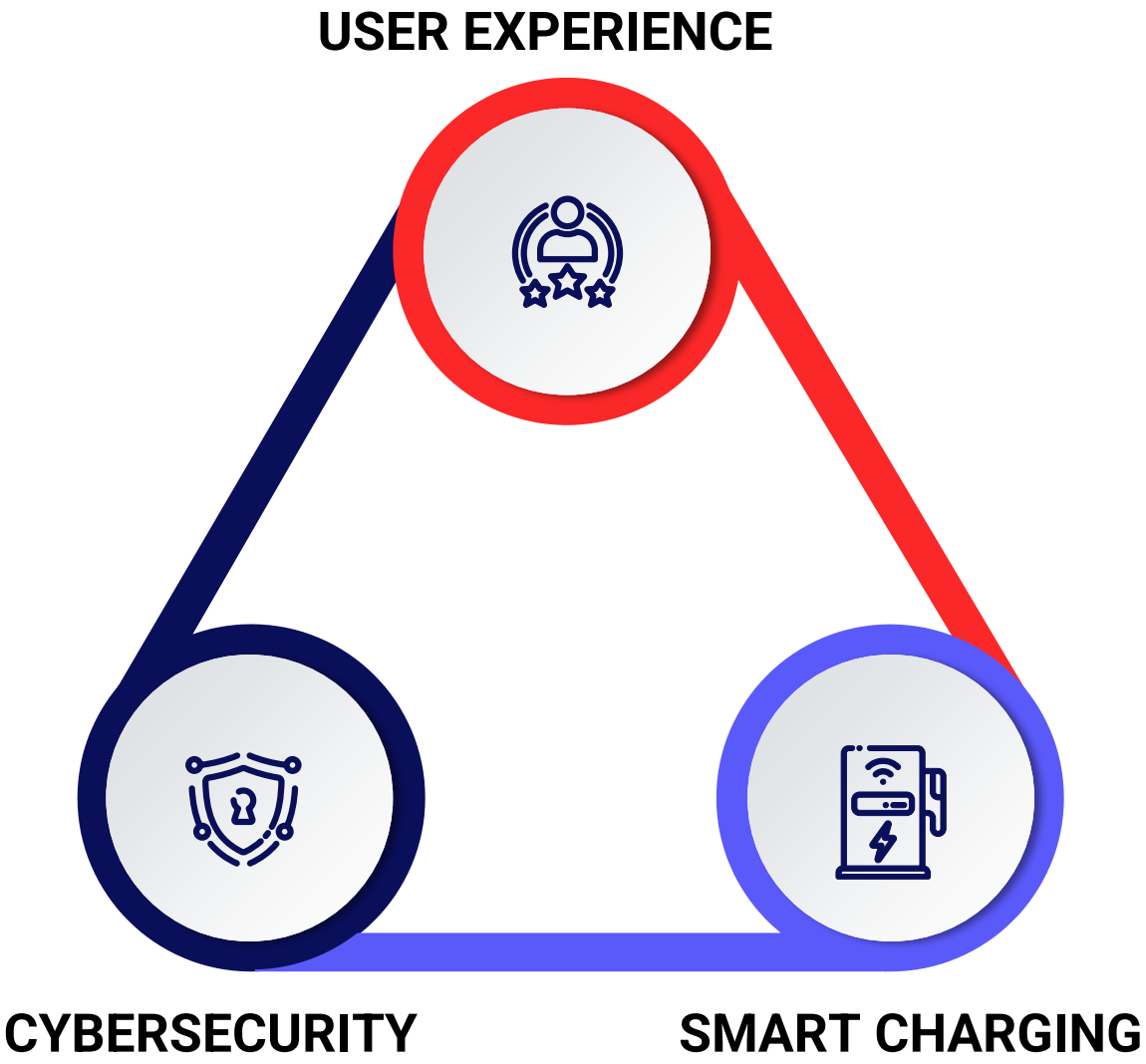
VISIT MOBENA.ORG FOR MORE INFORMATION

INSTITUT VEDECOM

Understanding Plug & Charge :

Why the service is valuable ?

Three main advantages



mobena

Next generation EV charging

How the service works ?

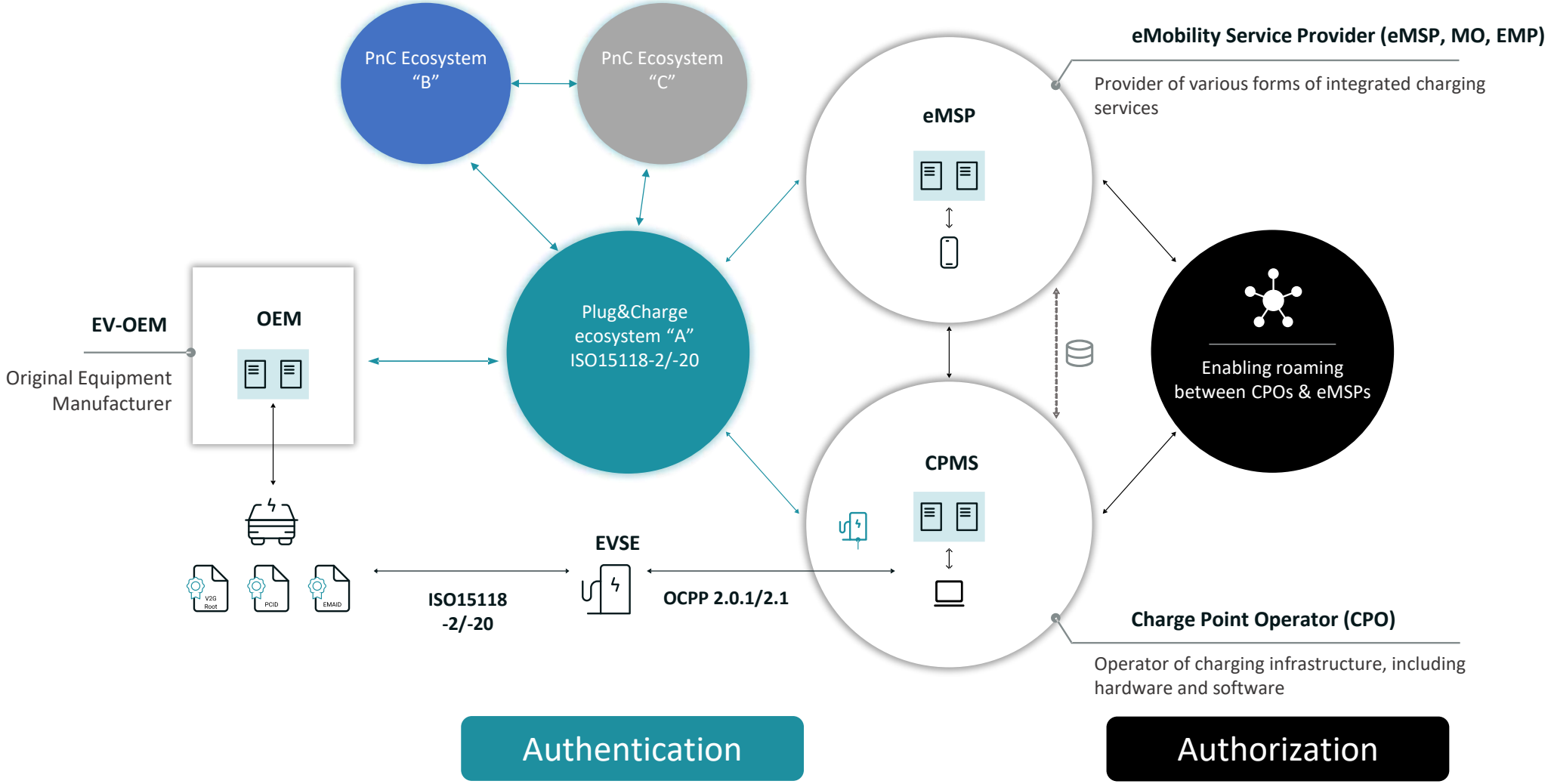
VISIT MOBENA.ORG FOR MORE INFORMATION

INSTITUT VEDECOM

Understanding Plug & Charge :

How the service works ?

Plug & Charge and eRoaming ecosystem at a glance



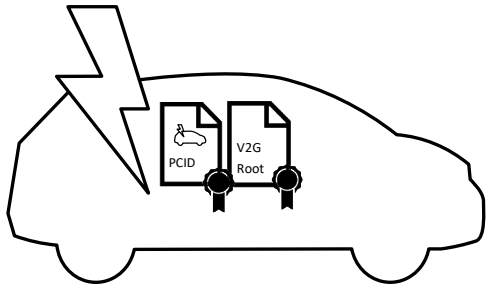
Understanding Plug & Charge :

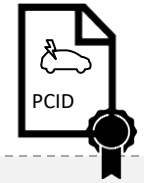
How the service works ?

OEM Provisioning Certificate and PCID Publication (OEM Responsibility)

1 Vehicle Production

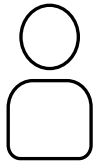
2 Publishing of Provisioning Certificate & Announcing PCID to Customer



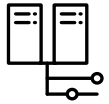


PCID via API

PCP



EV Owner



MO

Understanding Plug & Charge :

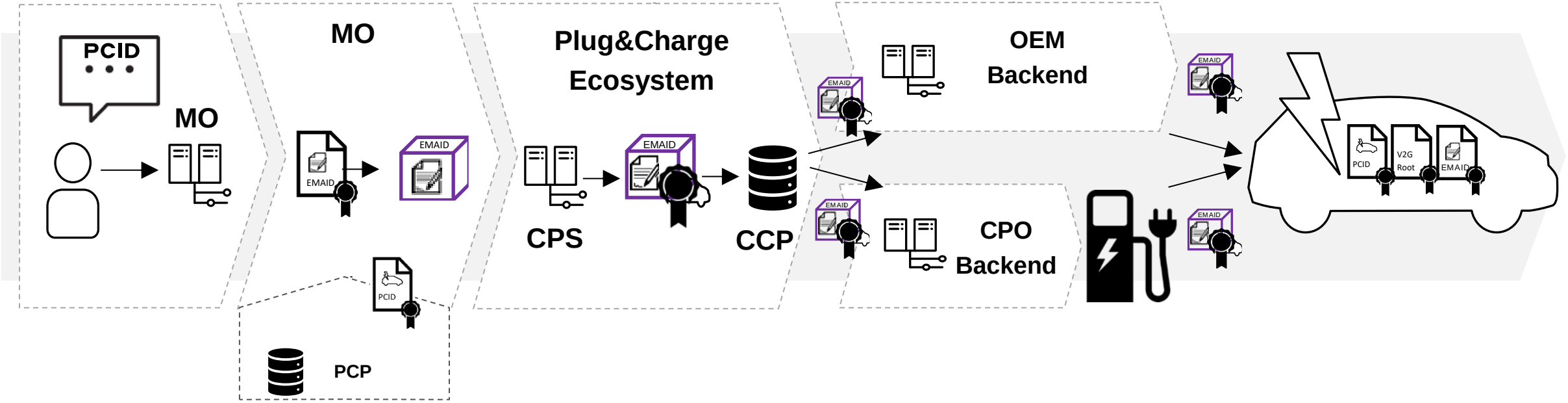
How the service works ?

Contract Generation, Signature and Installation

1 Creation of PnC Contract

2 Deliver Contract

3 Install Contract

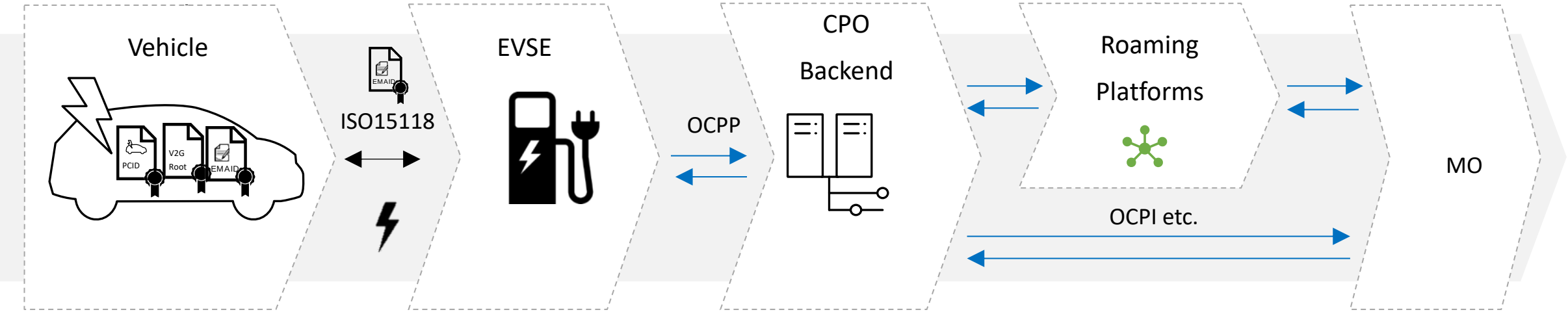


Understanding Plug & Charge :

How the service works ?

Authenticate and Authorize Charging Session

1. Authenticate at Charging Station
2. Authorize at CPO Backend
3. Authorize at Roaming Platforms and others
4. Authorize at MO Backend



Plug & Charge

Contract Certificate Validation

Contract Authorization

mobena

Next generation EV charging

What is the market status ?

VISIT MOBENA.ORG FOR MORE INFORMATION

INSTITUT VEDECOM

Understanding Plug & Charge :

What is the market status ?

The story so far with Plug & Charge worldwide

+70%

Global Auto OEMs chose implement ISO15118-2 Plug&Charge

2.6 million

PnC capable EVs on the road

7000+

Charging stations enabled PnC in EU

30%

Average quarterly increase of PnC sessions since 2019

Numbers based on Hubject Plug & Charge Ecosystem

Understanding Plug & Charge :

What is the market status ?

Major emobility players are already plugged into the Plug & Charge ecosystem

EV Producers (OEM)

CUPRA, Volkswagen, KIA, Porsche, Audi, Nissan, Lucid, Ford, VinFast, Hyundai, Scania, Renault Group, BMW Group, MINI, Genesis, MAN, Mercedes-Benz, smart, Polestar, Volvo, Stellantis, Skoda

Mobility Operators

Digital Charging Solutions, octopus ELECTROVERSE, Plugsurfing, nor+he, SMART/LAB, e·on, Ford, MONTA, VIRTA, BOSCH, IBIL Charging Technology and Services, carge, DEFTPOWER, Porsche, autoSense, SMATRICS, ev way, Elli, chargecloud, PLUGIT, AMPECO, EKO ENERGETYKA, CEPSA, zunder, TARDIS Technology, evconnect

Charge Point Operators (CPO)

mer, Longship.io, VIRTA, SMART/LAB, blink, bppulse, Porsche, electrify america, electrify canada, Shell Recharge, driivz, zunder, IONITY, be ENERGISED, IBIL Charging Technology and Services, BayWa, BOSCH, e·on, COMPLEO, enel way, Allego, Switch, sdey, EVGATEWAY, SMATRICS, greenflux, CHARZIN, ev way, Grid & Co., EKO ENERGETYKA, CEPSA, Spirii, AMPECO, EVgo, Lynkwell, AUTEL Powering the Planet, PLUGIT, XCHARGE, TARDIS Technology, evconnect, FRANCIS ENERGY

Charge Point Manufacturers (EVSE)

Certified

hypercharger by alpitronic, i-charging, KEMPOWER, AUTEL Powering the Planet, EVTEC, DELTA, EKO ENERGETYKA, Schneider Electric, StarCharge

Capable

TRITIUM, intech, Porsche Engineering, ABB, Zaptec, eSYSTEMS A KATEK Brand, ebee, ALFEN, BTC POWER, chargebyte

Understanding Plug & Charge :

What is the market status ?

Plug & Charge Adoption Worldwide – Capable EVs in the global market in the ecosystem

e.g. ID.x series

iX, i7, i5

e.g. Lucid Air

e.g. eTron, etron GT, MEB EVs

e.g. Ioniq series

e.g. VF7, VF8..

e.g. Enyaq

e.g. Cupra Born

e.g. EV8

e.g. Polestar 3

e.g. Taycan

e.g. City Lion E

e.g. GV60/70/80

e.g. Renault 5

e.g. Mach-E, E-Transit

e.g. EQE, EQS, EQA, PHEV

e.g. EX90

e.g. ...

AGENDA :

1 Understanding Plug & Charge

2 **Ensuring Interoperability**

3 Implementation Requirements

4 The future of Plug & Charge

mobena

Next generation EV charging

Role and value proposition of PKI

VISIT MOBENA.ORG FOR MORE INFORMATION

INSTITUT VEDECOM

Ensuring interoperability

Role and value proposition of PKI

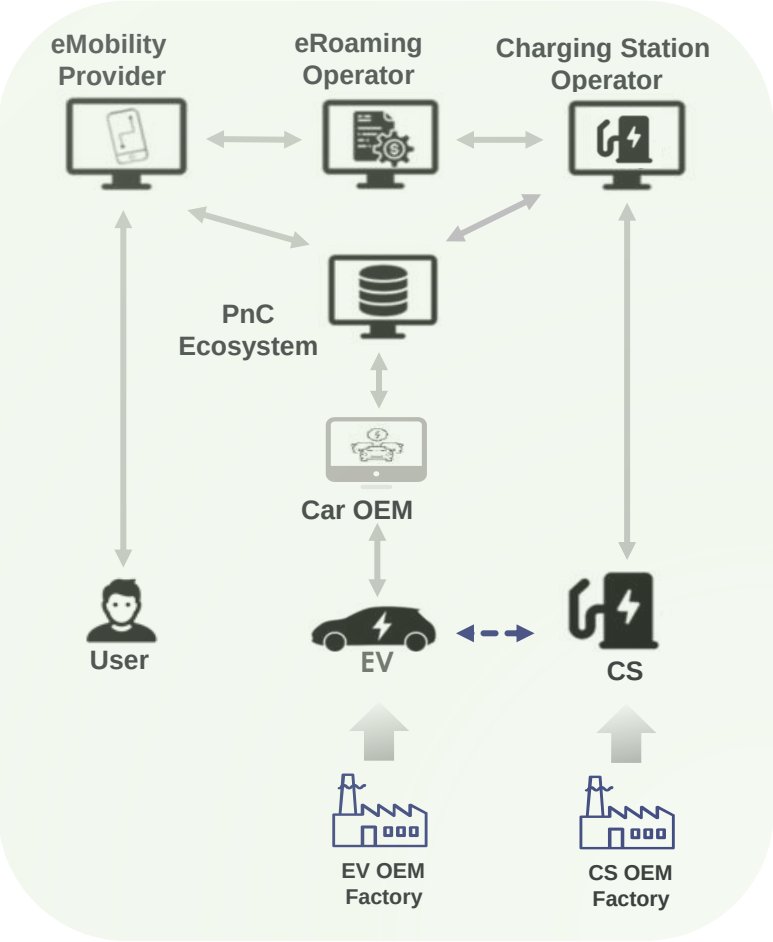
Context

- EV Charging Ecosystem involves several stakeholders with different roles and responsibilities, and devices belonging to different owners
  - Electro Mobility Providers, Charging Station Operators, eRoaming Operators, Charging Station Manufacturers, EV Manufacturers, and their respective Server applications.
  - Electric Vehicles (EV), Charging Stations (CS).
  - EV users.

- Interoperability and trust between all these entities is a must
  - To protect assets and business of each actors
  - To deliver EV Charging Service with high quality, up and running, and best user experience levels.
  - To sustain transition to Electric Vehicle widely in Europe.

- European Parliament voted Cyber Resilient Act for IoT devices
  - To engage OEMs, distributors, resellers to implement cybersecurity measures from design to product end of life, to ensure the privacy and the protection of data and communications.

- ISO Standard (ISO15118) has chosen Public Key Infrastructure to secure EV Charging ecosystem and Plug and Charge feature
  - Why ?

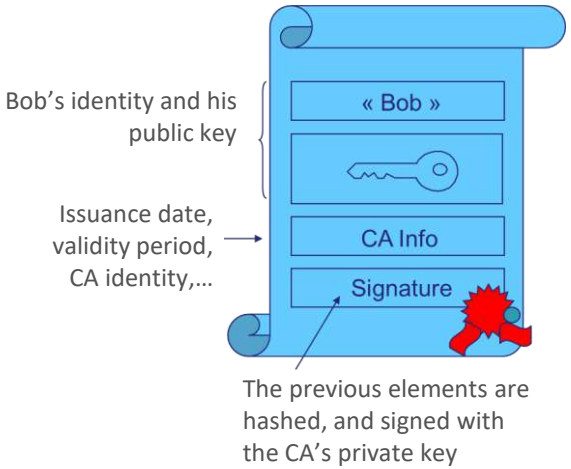


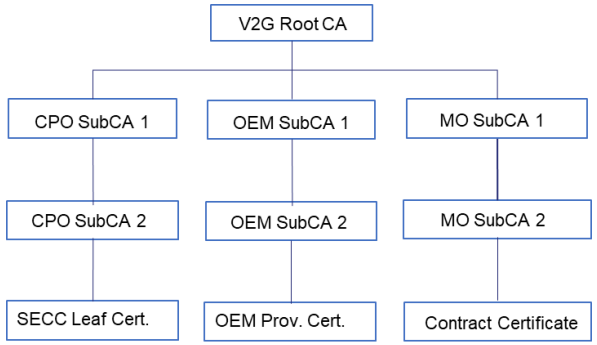
Ensuring interoperability

Role and value proposition of PKI

Public Key Infrastructure - Basics

- **PKI is a framework** designed to manage digital security by using cryptographic techniques and digital certificates, to ensure identity verification and secure communication.
- **Its core components** are:
  - **An asymmetric key pair** made of a Private key kept secret and a Public Key openly shared.
    - Private Key is used to compute digital signature, or to decrypt data. Shall be generated and stored in a Secure Element on the charging station side. And in a Hardware Secure Module for the Server side.
    - Public Key is used to verify digital signature, or to encrypt data.
  - **A digital certificate:** A digital document that binds a public key to an entity's identity, containing information of the certificate holder (name, serial number, pubkey, validity date…).
  - **The Certificate Authority** verifies certificate holder identity, before issuing the Certificate. It ensures that the public key included in the certificate belongs to the entity it claims to represent.
  - **A Certificate Revocation List / Online Certificate Status Protocol** published by the CA that contain serial numbers of certificates that have been revoked before their expiry date.
  - **A Trust Hierarchy** organized as a tree where:
    - Root CA is the top-most CA in the PKI hierarchy, trusted by default and often embedded in software or hardware systems. It issues certificates to intermediate CAs.
    - Intermediate CAs : CAs that are subordinate to the Root CA and issue certificates to end entities or further intermediate CAs.
    - End Entities (or Leaves) : The final recipients of certificates, such as users, devices, or servers, whose public keys are bound to their identities.
- **A Digital Signature** is used to perform authenticity and integrity verification of the message.





Ensuring interoperability

Role and value proposition of PKI

- PKI provides a structured ecosystem with roles, policies, and procedures to create, manage, use, store, revoke, renew digital certificates, cryptographic keys, perform digital signature, ensuring secure and trusted interactions between entities, based on :
  - **Authenticity :** Validates the identity of entities involved in the communication.
  - **Integrity :** Confirms that data has not been tampered with during transmission.
  - **Confidentiality :** Ensures that communication and data are encrypted and secure.
  - **Non-repudiation :** Provides evidence that a particular entity performed a specific action

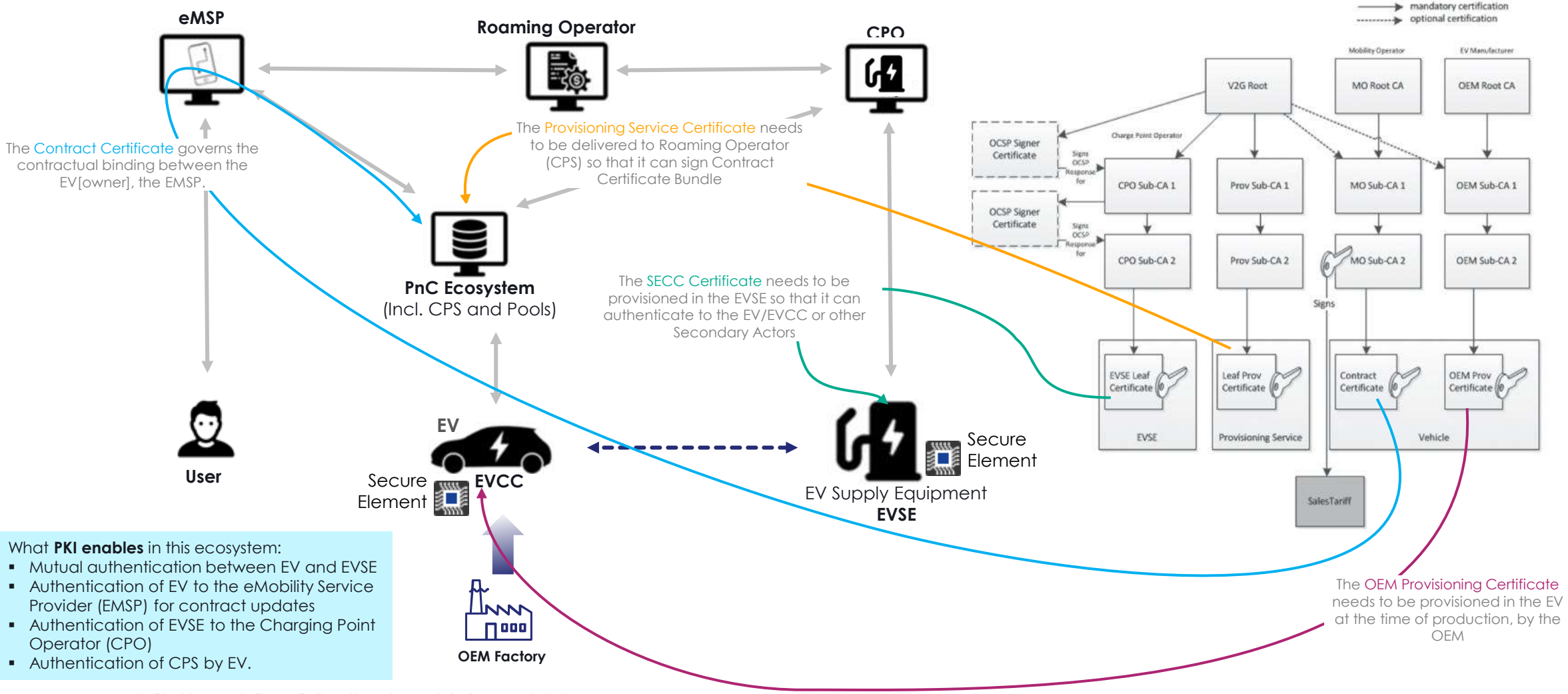
- Indirectly, PKI provides
  - **Interoperability :** Beyond the protocol aspects, in Multi-PKI providers context, Certificate Trust List ensures that all entities communicate with trust.
  - **Scalability :** The hierarchical approach allows for scalable and manageable certificate issuance.
  - **Service Resilience :** Expired or revoked Certificates can be renewed.

- PKI benefits applies to the EV Charging ecosystem entities, the Contract Certificate creation and distribution process.
- Without PKI, it would have been complex to authenticate the parties, secure the communications, check the certificates origin, binds the contract certificate to a unique EV.

Ensuring interoperability

Role and value proposition of PKI

PnC – PKI as a cornerstone of ISO 15118



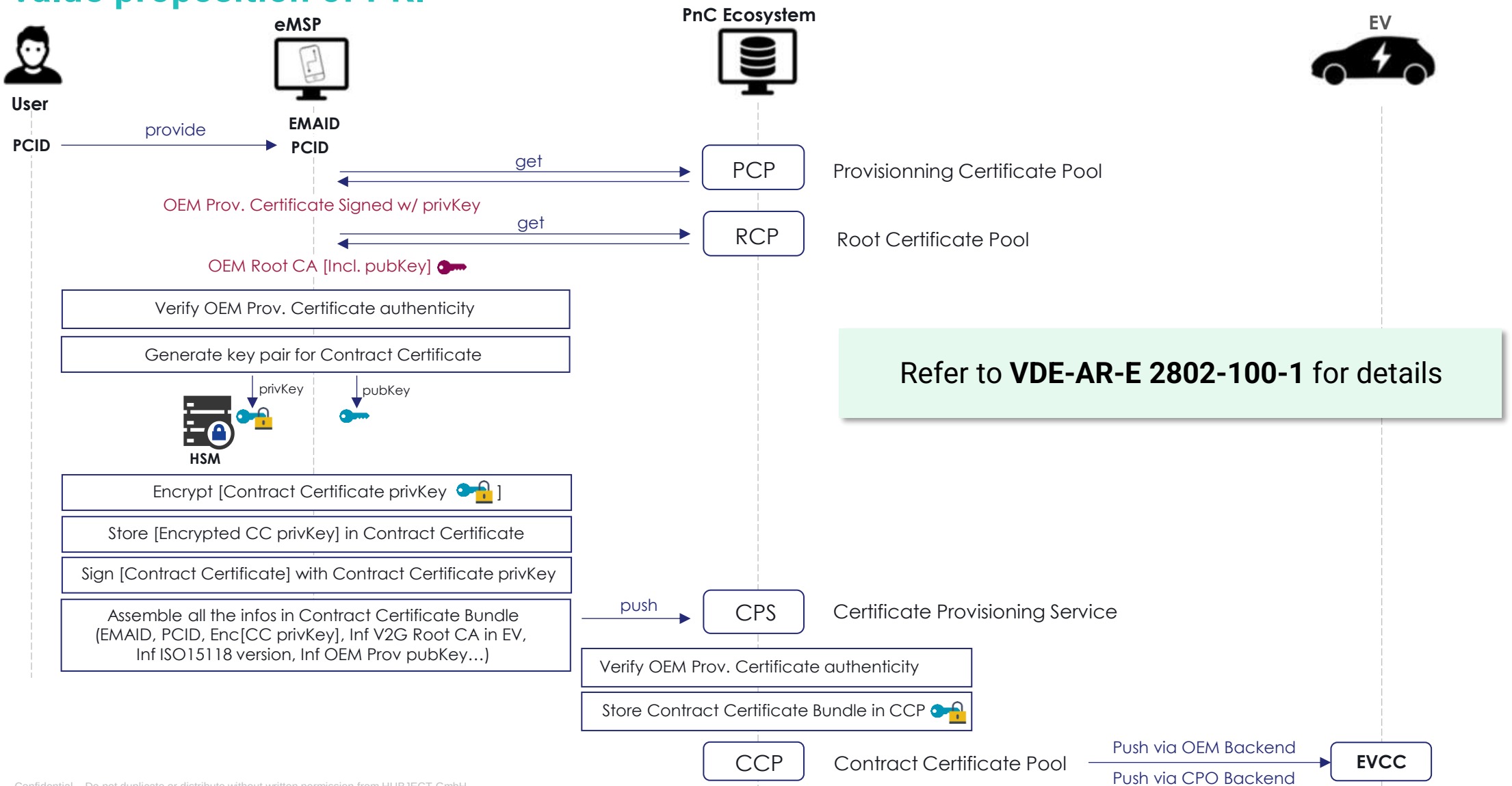
What **PKI enables** in this ecosystem:

- Mutual authentication between EV and EVSE
- Authentication of EV to the eMobility Service Provider (EMSP) for contract updates
- Authentication of EVSE to the Charging Point Operator (CPO)
- Authentication of CPS by EV.

Ensuring interoperability

Role and value proposition of PKI

PnC – Contract certificate distribution



Refer to **VDE-AR-E 2802-100-1** for details

mobena

Next generation EV charging

Interoperability

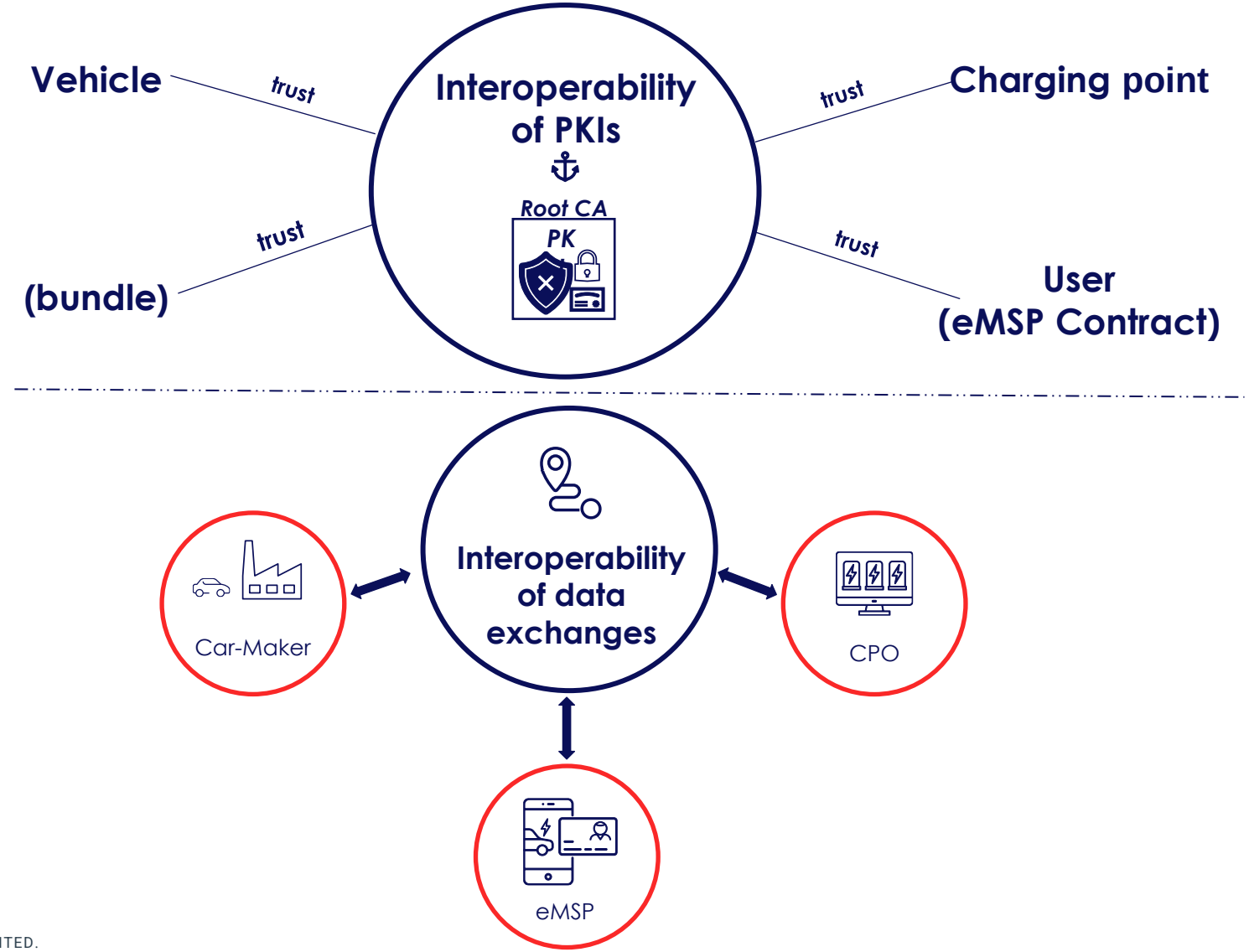
VISIT MOBENA.ORG FOR MORE INFORMATION

INSTITUT VEDECOM

Ensuring interoperability

STF groups : Interoperability as a founding principle

A basic principle: any EV-Driver must be able to charge any EV (whatever the car maker), on any charging station (whatever the charger maker, whatever the CPO, whatever the country), using any service provider (whatever the eMSP)”



Ensuring interoperability

Highlight interoperability issues to ensure a trustworthy market

A basic principle: any EV-Driver must be able to charge any EV (whatever the car maker), on any charging station (whatever the charger maker, whatever the CPO, whatever the country), using any service provider (whatever the eMSP)”

Interoperability between EV, EVSE	Comm. : ISO 15118 (but we must pay attention to “-2” and “-20” coexistence) Trust : List of V2GRootCAs in the EV trust-store (and behind, OEM Back-ends, RootCA-Pools and Trust-Lists)
Interoperability between CPO, eMSP	Trust : List of MORootCAs in the CS/CPO trust-store (and behind, CPO Back-ends, RootCA-Pools and Trust-Lists) Authorisation : Roaming (This topic is Key, but well-known and fully separated from PKI and P&C topics)
Interoperability between Back-ends CPO, eMSP, OEM	Data exchanges 1 : Pools and P&C PKI ecosystems (these systems exist for exactly that.) Data exchanges 2 : Inter-Pools interop. (Feasibility is OK – proved by Mobena – Topology architecture and business solution definition is in progress. A need for inter-pool protocol definition)
Interoperability between EV Driver, EV, Multi-eMSP contracts	CC installation : CarMaker-OEM must allow the CC installation whatever the MO/eMSP + List of V2GRootCAs in the EV trust-store CC selection/prioritization : CarMaker-OEM must allow CC selection/prioritization on board (or via a smartphone app)**It must be ensured this is done with the explicit consent of the User**

Ensuring interoperability

Multi V2G/MO/OEM-PKI-Compatibility

EV OEMs

Used for TLS & Contract Bundle Installation

1. Reserve memory in EV for V2G-Roots
2. be able to install & update V2G Root
3. Be able to identify trusted players
   - CTL
   - Local Root Certificate Pools
   - Manual V2G-Root Selection of the Market

EVSE manufacturer and CPOs

Used for Contract Certificate Authentication

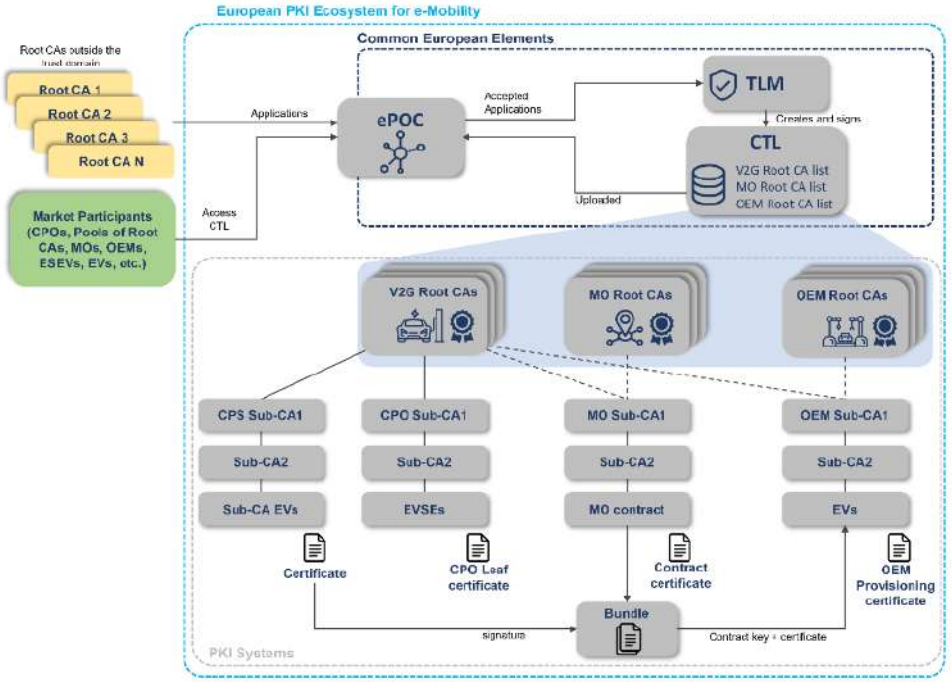
1. Reserve memory in EVSE for MO- and V2G-Root
2. be able to install & update MO- and V2G-Root
3. Be able to identify trusted players
   - CTL
   - Local Root Certificate Pools
   - Manual V2G-Root Selection of the Market

PKI Operators

V2G/MO/OEM Root

1. Publish Certificate Policy publicly
2. To be in CTL: comply / apply to IT Security Guideline and Certifications defined by
   - STF in EU
   - SAE in US

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



mobena

Next generation EV charging

P&C ecosystem Providers

VISIT MOBENA.ORG FOR MORE INFORMATION

INSTITUT VEDECOM

Ensuring interoperability

Plug & Charge ecosystem providers

Ecosystems – market overview

What is an ecosystem ?

- Concept used in STF
- Pool + PKI providers

At the EU level :

- Different providers
  - Hubject
  - Gireve
  - *CharIN & irdeto soon*

Rest of the world
The market is evolving :

- EU players developing worldwide
- Initiatives worldwide:
  - SAE in the US
  - Autocrypt in Asia

The agenda :

1 Understanding Plug & Charge

2 Ensuring Interoperability

3 **Implementation Requirements**

4 The future of Plug & Charge

mobena

Next generation EV charging

How do eMSPs, CPOs and OEMs enable P&C ?

VISIT MOBENA.ORG FOR MORE INFORMATION

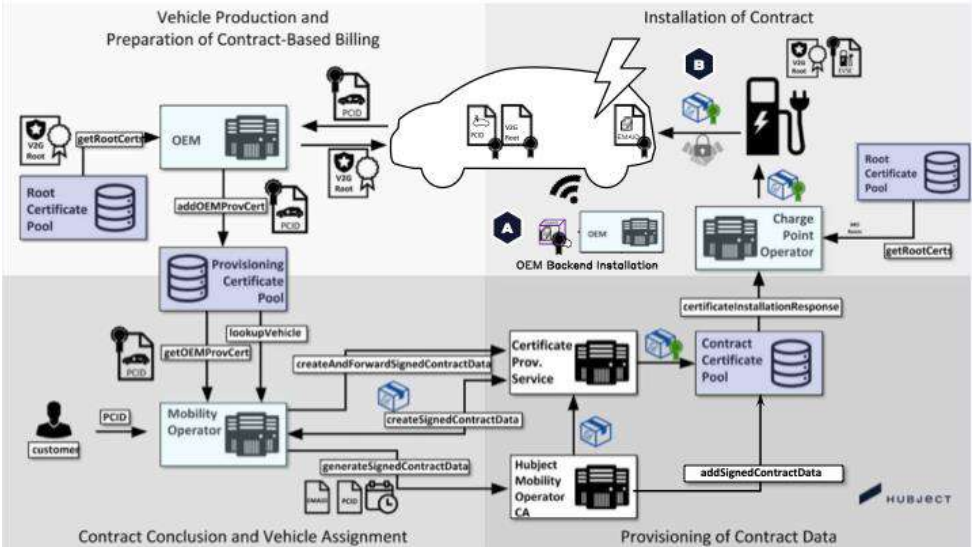
INSTITUT VEDECOM

Implementation requirements

What eMSP's, CPOs (& OEMs) have to do to offer the service ?

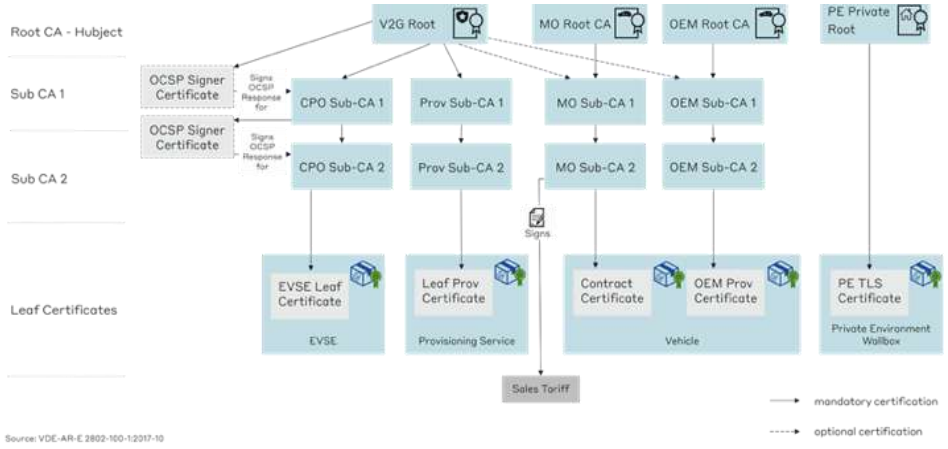
Two technical dimensions need to be considered :

PnC ECOSYSTEM



The PnC ecosystem is providing certificate pools and API connections for the Ecosystem partners to access the pools and services. It manages the certificates, i.e. manage, store, move and delete certificates on behalf of our PnC ecosystem partners.

V2G, MO AND OEM ROOT PKIS



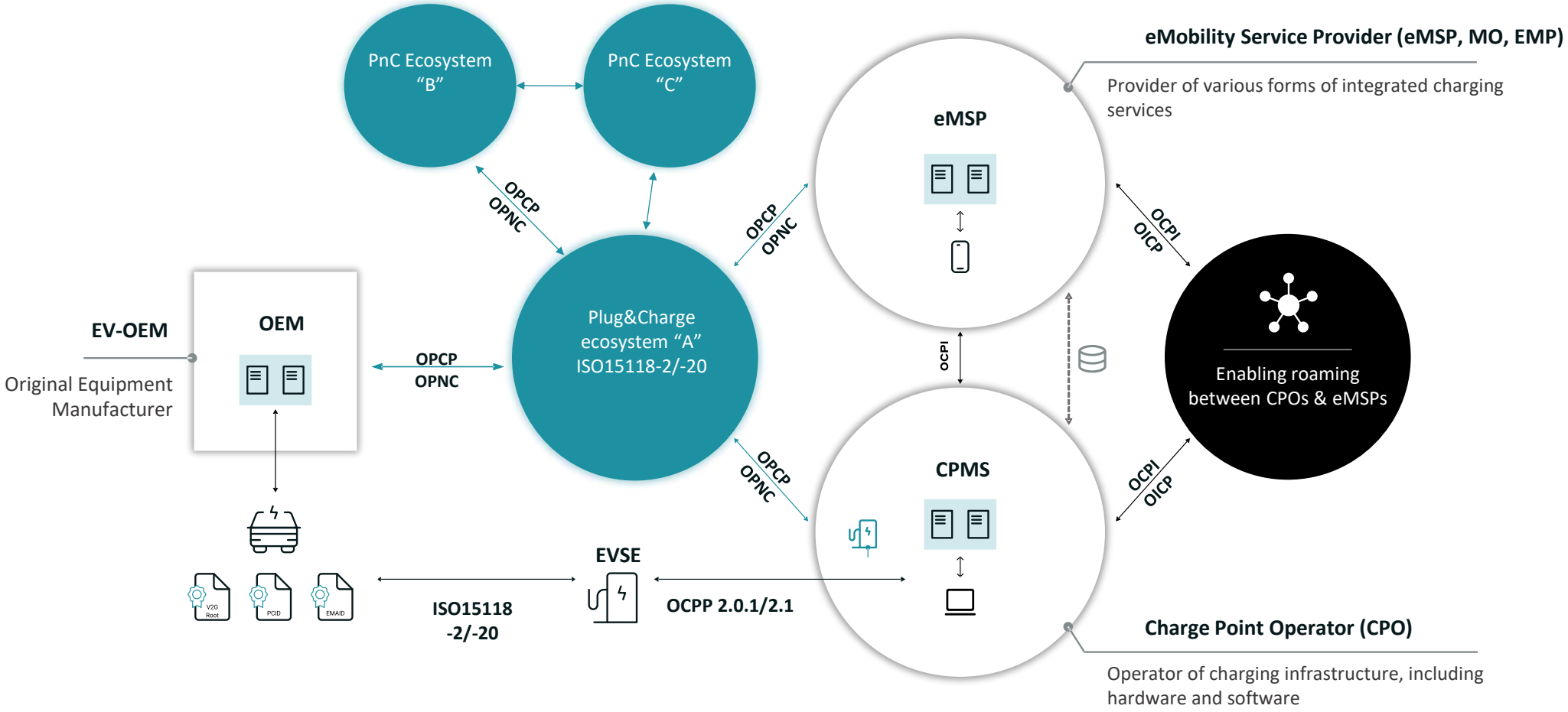
Which are the main certificates that are existing?

ORIGINAL EQUIPMENT MANUFACTURER (OEM)	CHARGE POINT OPERATOR (CPO)	MOBILITY OPERATOR (MO)
Provisioning Certificates	EVSE Certificates	Contract Certificates

Implementation requirements

What eMSP's, CPOs (& OEMs) have to do to offer the service ?

Plug & Charge and eRoaming ecosystem at a glance



Implementation requirements

What eMSP's, CPOs (& OEMs) have to do to offer the service ?

Politics and Governance

CPO

Hardware compatible?

- Yes → Software compatible?
- No → Talk to your supplier, we can support there! → Software compatible?

Software compatible?

- No → Implement OCPP OCA / 2.0.1
- Yes → Connect to your Plug&Charge Ecosystem

MO

Use own MO Root

- Yes → Setup own MO PKI
- No → Connect to your Plug&Charge Ecosystem

OEM

Support with

- Software requirements
- Hardware requirements
- Setup of an PKI (optional)
- E2E Testing

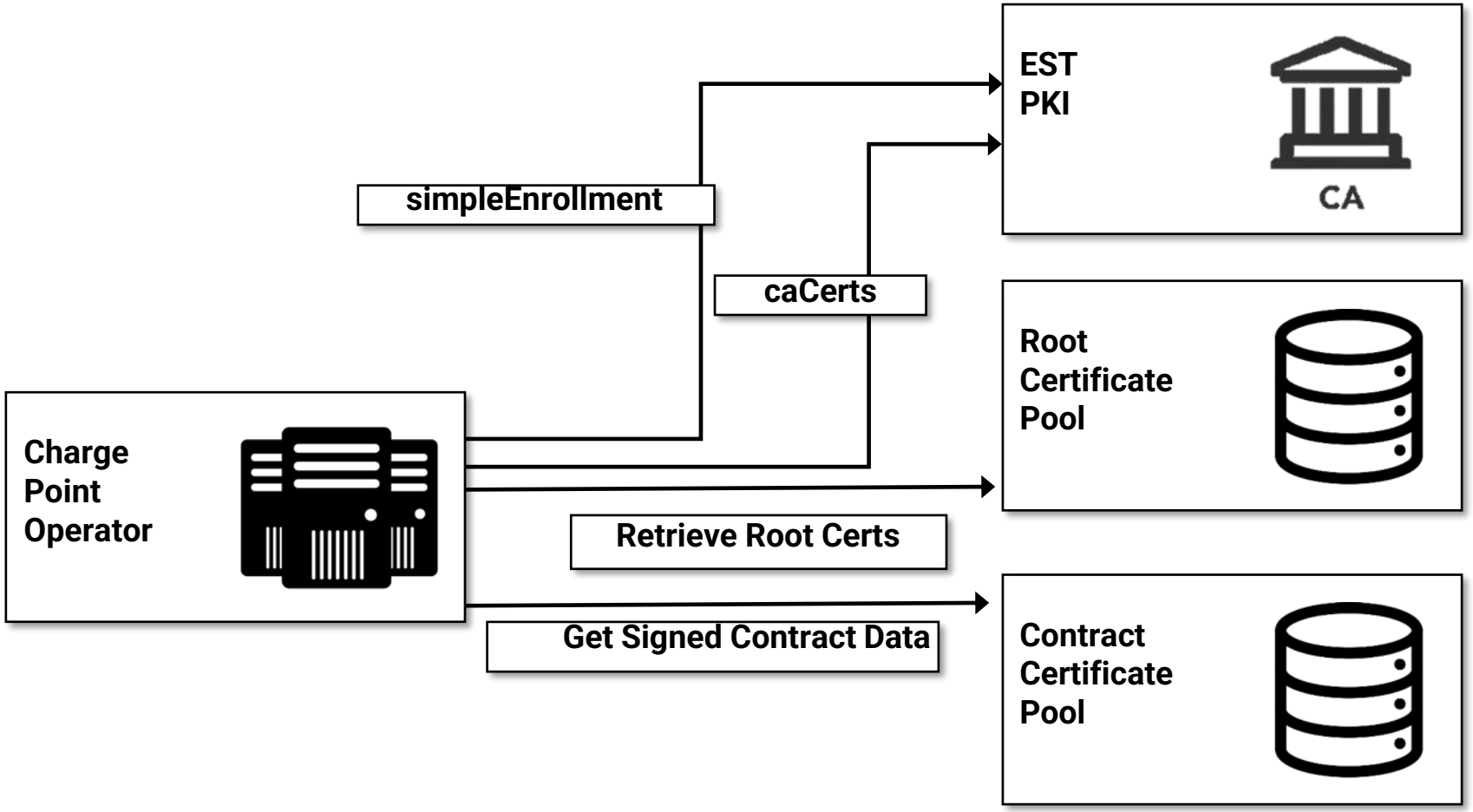
Connect to your Plug&Charge Ecosystem

Plug&Charge is now!

Implementation requirements

What eMSP's, CPOs (& OEMs) have to do to offer the service ?

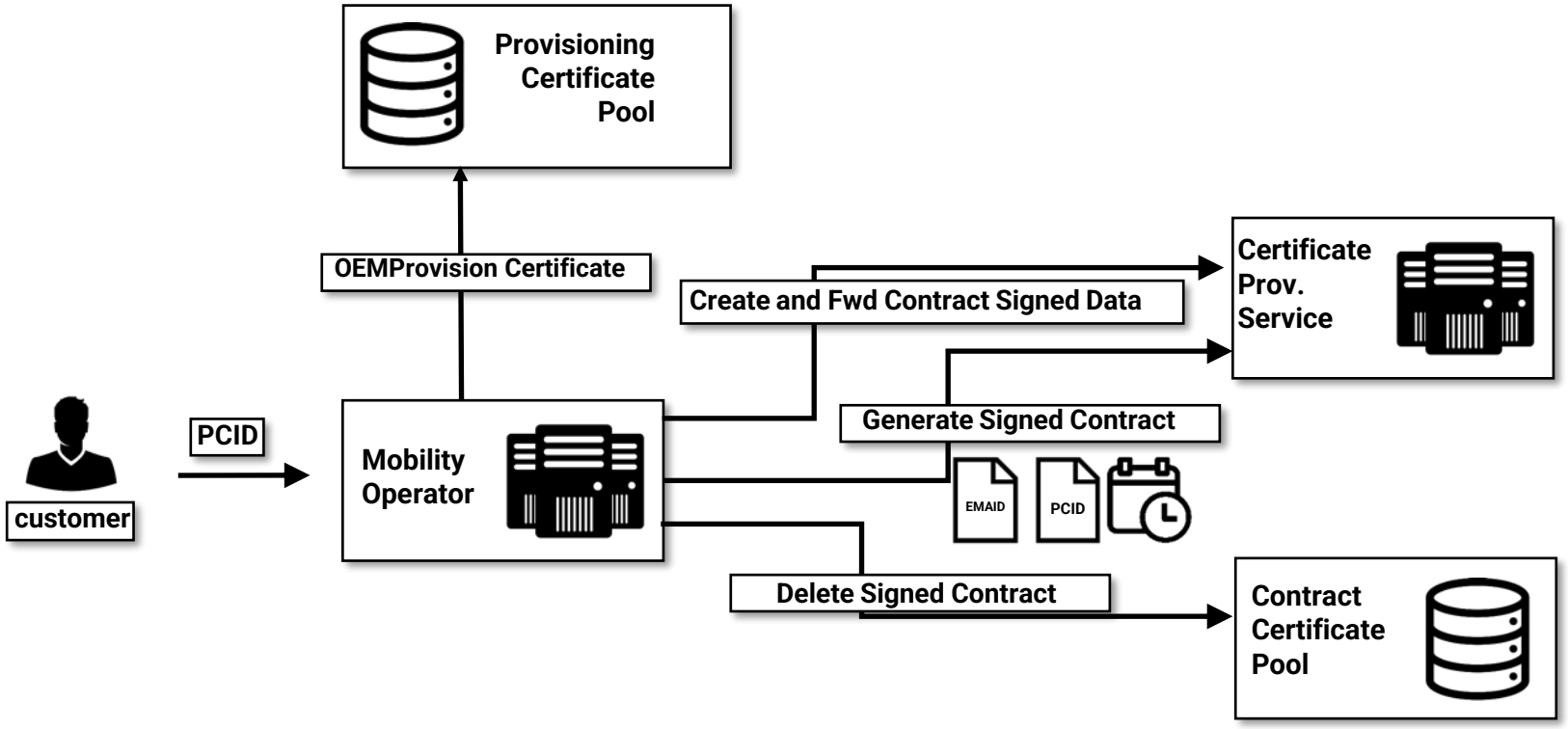
The CPO needs to implement four interfaces

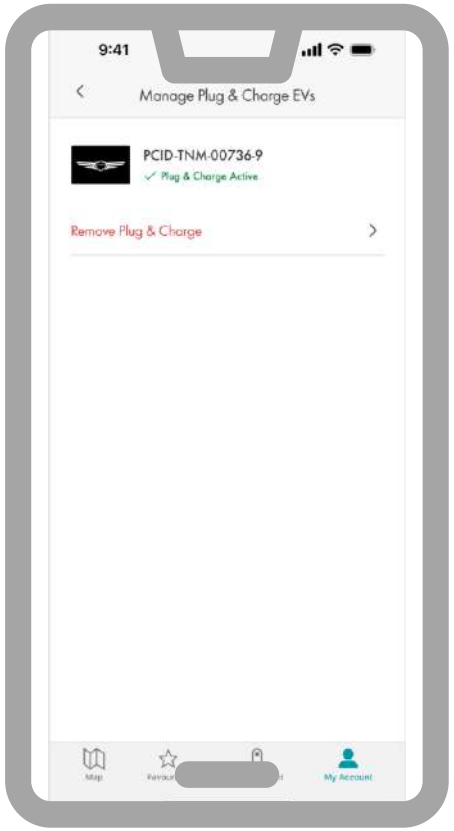


Implementation requirements

What eMSP's, CPOs (& OEMs) have to do to offer the service ?

MO needs to implement two Interfaces to the ug & Charge ecosystem (using Hubject PKI Service)



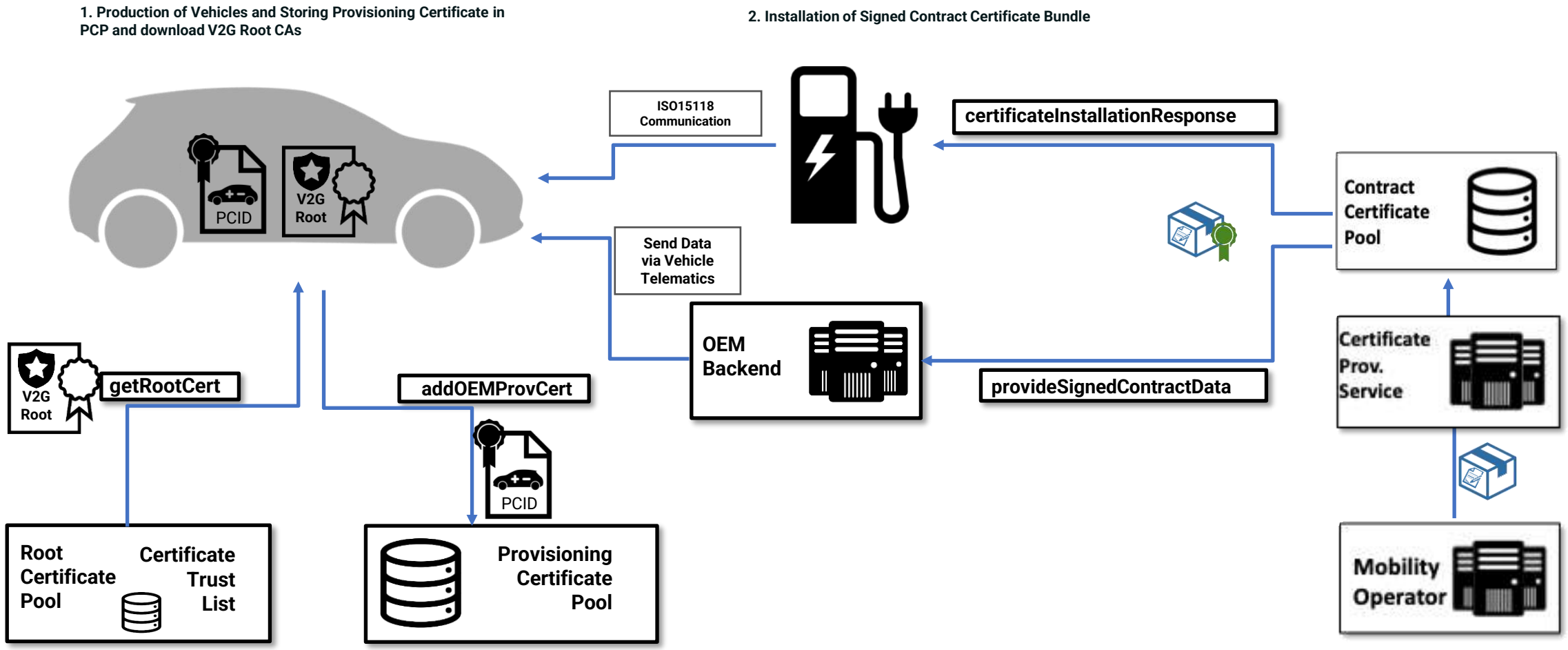


Example

Implementation requirements

What eMSP's, CPOs (& OEMs) have to do to offer the service ?

OEM needs to implement two to four Interfaces to connect to a Plug & Charge ecosystem



mobena

Next generation EV charging

Testing P&C from SIL to HIL to ensure conformity and interoperability

INSTITUT VEDECOM

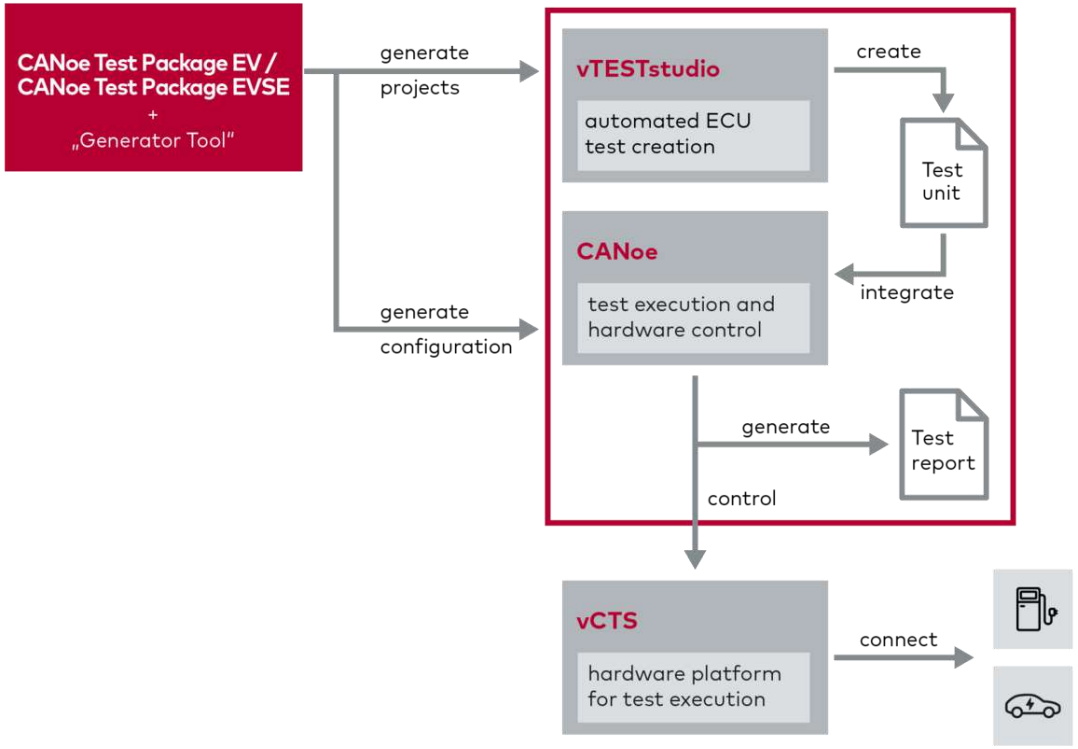
VISIT MOBENA.ORG FOR MORE INFORMATION

Implementation requirements

Conformance and Interoperability Tests for PnC According To ISO 15118

CANoe Test Package EV provides **conformance/interoperability** tests for **electric vehicles**

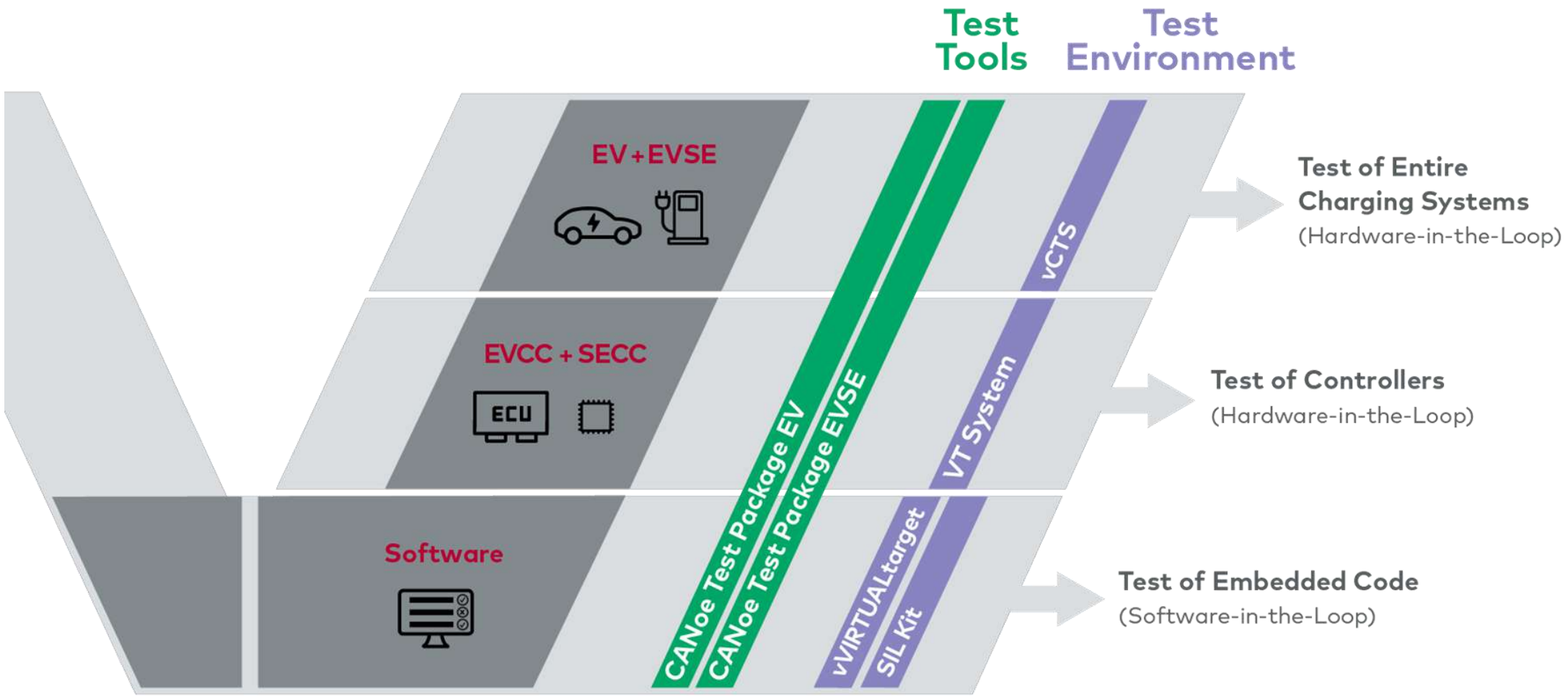
CANoe Test Package EVSE provides **conformance/interoperability** tests for **charging stations**



- Includes test cases for PnC according to ISO 15118-4
- Delivery includes source code
- Saves the Master Secret for TLS encryption in the log file

Implementation requirements

Testing PnC from SIL to HIL



Implementation requirements

HIL Testing With VT System

VT System

- Simple connection of the I/O interfaces of the ECU
- Minimal wiring effort for test setups
- Seamless integration into CANoe

- Execution of the **CANoe Test Package EV/ EVSE**

- Use Case:
  - ECU and Controller Tests.
  - Build own test system (HIL)

Implementation requirements

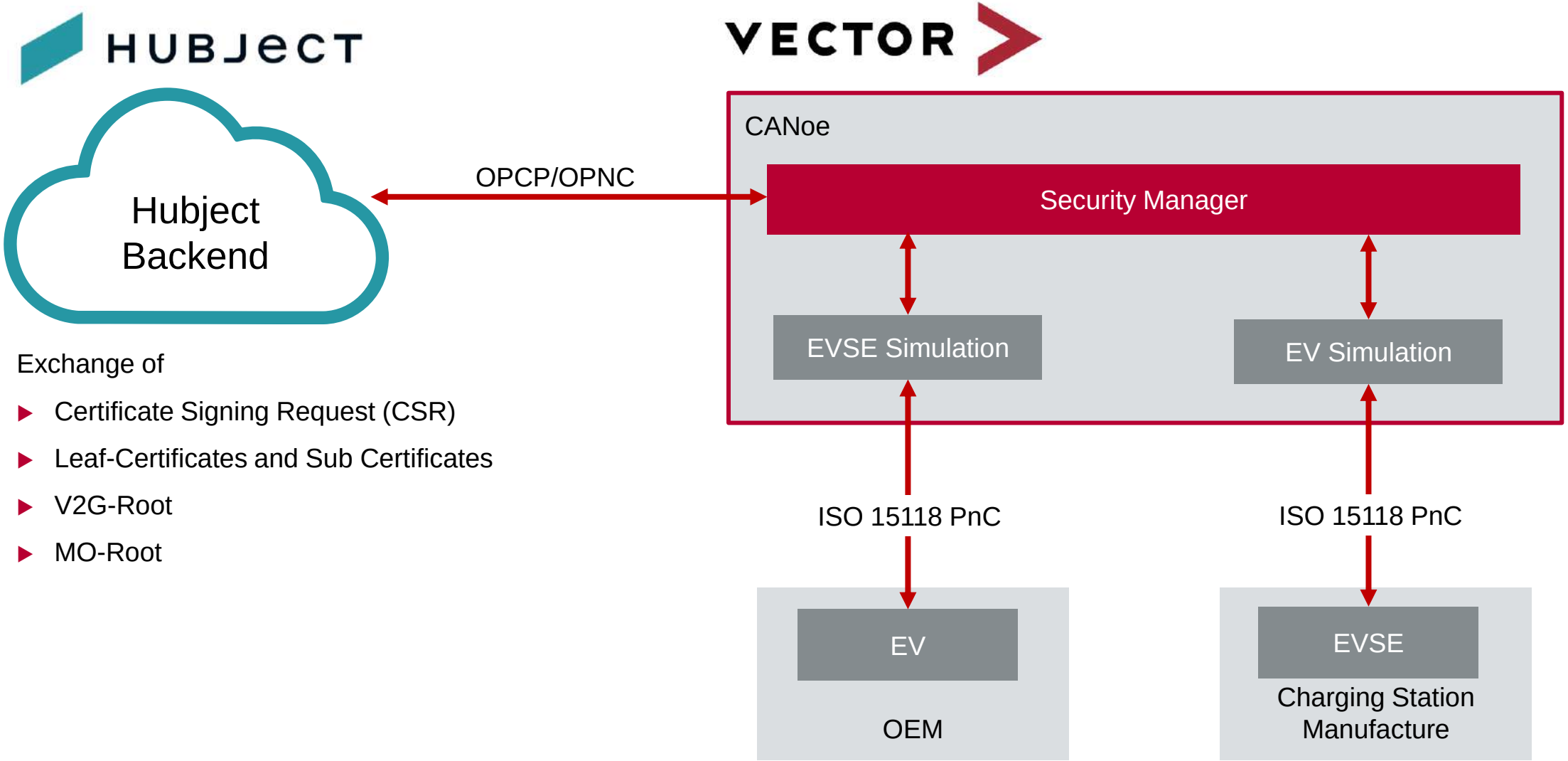
HIL Testing With vCTS

Vector Charging Test System (vCTS)

- Optimized hardware platform for execution of tests with **CANoe Test Package EV/ EVSE**
- Flexible adaptation to tested charging standards (CCS1, CCS2, GB/T, CHAdeMO and NACS)

Implementation requirements

Hubject PKI in Vector Tools

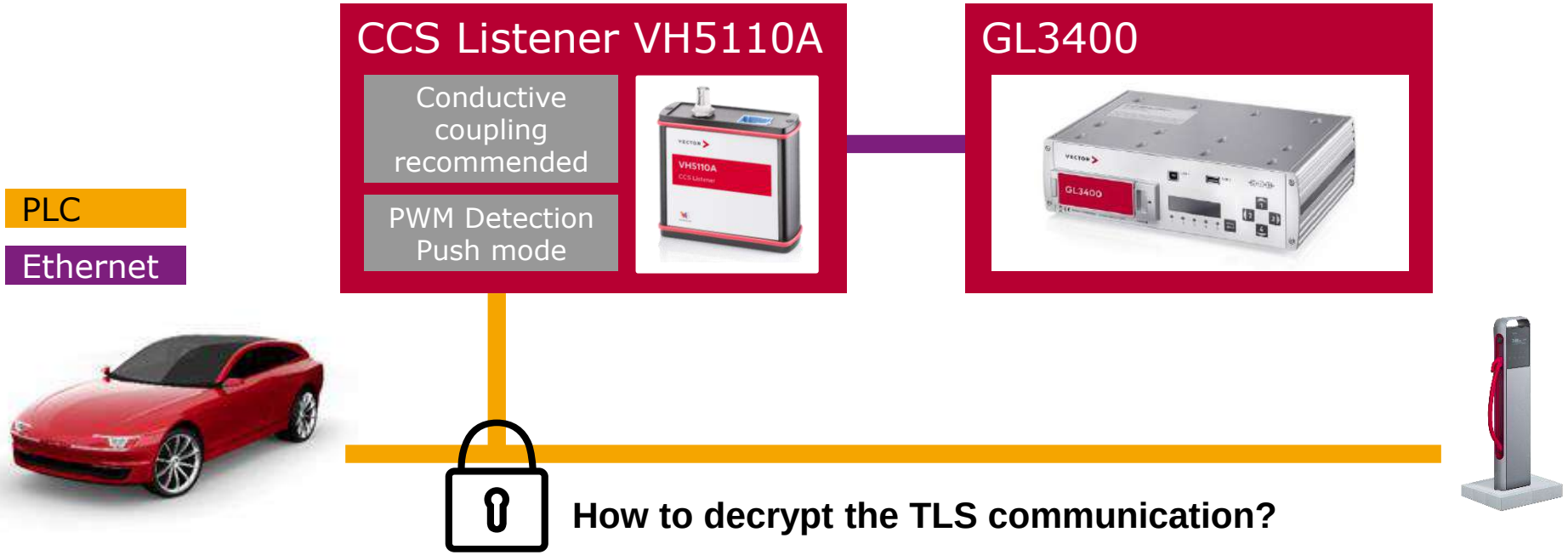


Exchange of

- Certificate Signing Request (CSR)
- Leaf-Certificates and Sub Certificates
- V2G-Root
- MO-Root

Implementation requirements

Decrypt TLS for PnC



How to decrypt the TLS communication?

- Set Master Secret manually in Vector Security Manager
- Set Master Secret via CAPL-Code in Vector Security Manager
- Transmit Master Secret via UDP-Frame

Implementation requirements

Summary – CANoe Test Package EV/EVSE

- **Testing over all integration levels**
  - Test your software stack with Software-in-the-Loop (SIL).
  - Test your ECU and EV or Charging Station with Hardware-in-the-Loop (HIL).

- **TLS Decryption**
  - CANoe saves the Master Secret in the log file that you and your partners can always decrypt the smart charging communication within CANoe.

- **Access internal bus communication**
  - Show your internal bus communication and diagnostic values of the ECU time synchronous with the smart charging communication in CANoe.

- **Delivery includes source code**
  - Easy creation of new custom specific test cases.

The agenda :

1 Understanding Plug & Charge

2 Ensuring Interoperability

3 Implementation Requirements

4 **The future of Plug & Charge**

mobena

Next generation EV charging

Plug & Charge is here to stay

Its place in payment solutions

VISIT MOBENA.ORG FOR MORE INFORMATION

INSTITUT VEDECOM

Future rollout of the Plug & Charge

Plug & Charge is here to stay – its place in payment solutions

- Increased Security compared to RFID or Autocharge
- All major global OEMs, MOs and CPOs are offering Plug&Charge today
- End Customers give great feedback to the feature and want to use it
- Legislation and Regulation are pushing and giving requirements for using ISO 15118 and Plug&Charge as mandatory
- Needed function to offer proper automated charing options, Bi-Directional Charging, Smart Charging
- Reduced costs for MSPs
- Great opporunity for Fleets, Depots or AC-Charging parks
- Enabler for value added services

mobena

Next generation EV charging

Regulation & STF results

VISIT MOBENA.ORG FOR MORE INFORMATION

INSTITUT VEDECOM

The future of Plug & Charge

Regulation &STF

EU REGULATIONS

European Transport Forum is working with market participants to synchronize legislative acts between charging infrastructure and EVs to specific issues concerned with the standard ISO15118.

SUSTAINABLE TRANSPORT FORUM:
SUBGROUP 1

INCENTIVES

As the **US NEVI* Program** defines ISO15118:2 and Plug&Charge as mandatory for EVSE Infrastructure, this is pushing Plug&Charge in North America.

In parallel the **transition to NACS** brings the TESLA Network into the PnC Discussion.

MARKET COLLABORATION

Several associations & working groups:

❖ **CharIN:**
- Defined **good practices** for CP
- Defined **standard vision** of use cases for P&C
- Works on a **standard protocol OPNC** for the market

❖ **Mobena:**
- Worked on **Plug & Charge deployment** in Europe
- Made **demos on pool interoperability**
- Published **business use cases** & **technical descriptions** for Plug&Charge implementation.

The future of Plug & Charge

Interoperability as a founding principle

Interoperability & Trust require common rules

Exchanges & contributions

STF PERIMETER	MOBENA PERIMETER
Trust requires the definition of **shared rules**	**Ensuring interoperability** requires sharing rules
Certificate Policy	Architecture, protocols
Security requirements	Use cases
Market Rules	Standard business player model
	Defined business objects

The future of Plug & Charge

PKI architectures

15118 deployment requires at least 1, probably several PKI named **“V2G Root CA”**. **The number of PKIs and how they co-exist** impacts the level of interoperability and market organisation.

- 4 scenarios were analysed & compared
- 1 scenario was chosen

An organisation based on the principle of several PKIs co-existing, regulated and federated through a Trust List.

The EU Commission has accepted to organise & maintain the regulation.

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

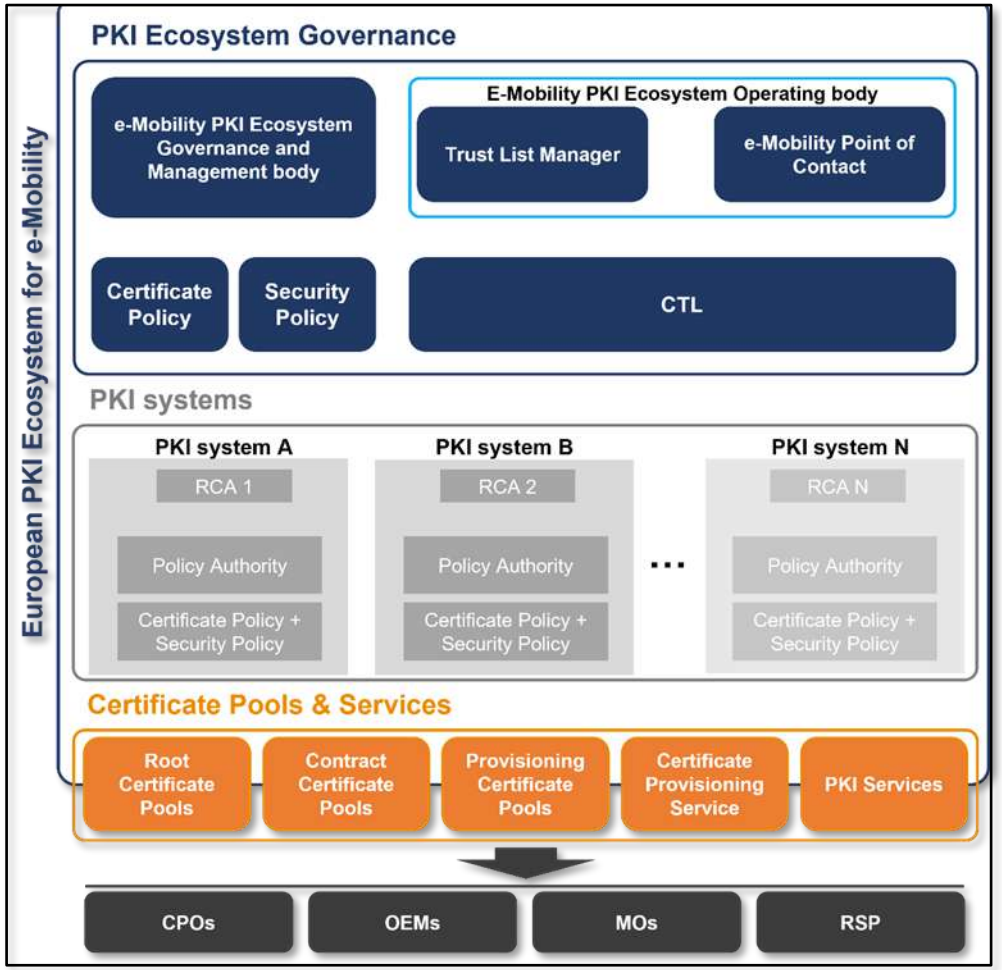
The future of Plug & Charge

STF Groups - Results

The EU PKI ecosystem is divided into 3 parts

- ❖ The regulated zone
  - Governance players
  - PKI operators
- ❖ The interface zone
  - Pool operators
- ❖ Emobility players and users

Deliverable 6 - Development of the architecture, governance, and operating models for a PKI under ISO 15118



Thank you for your attention