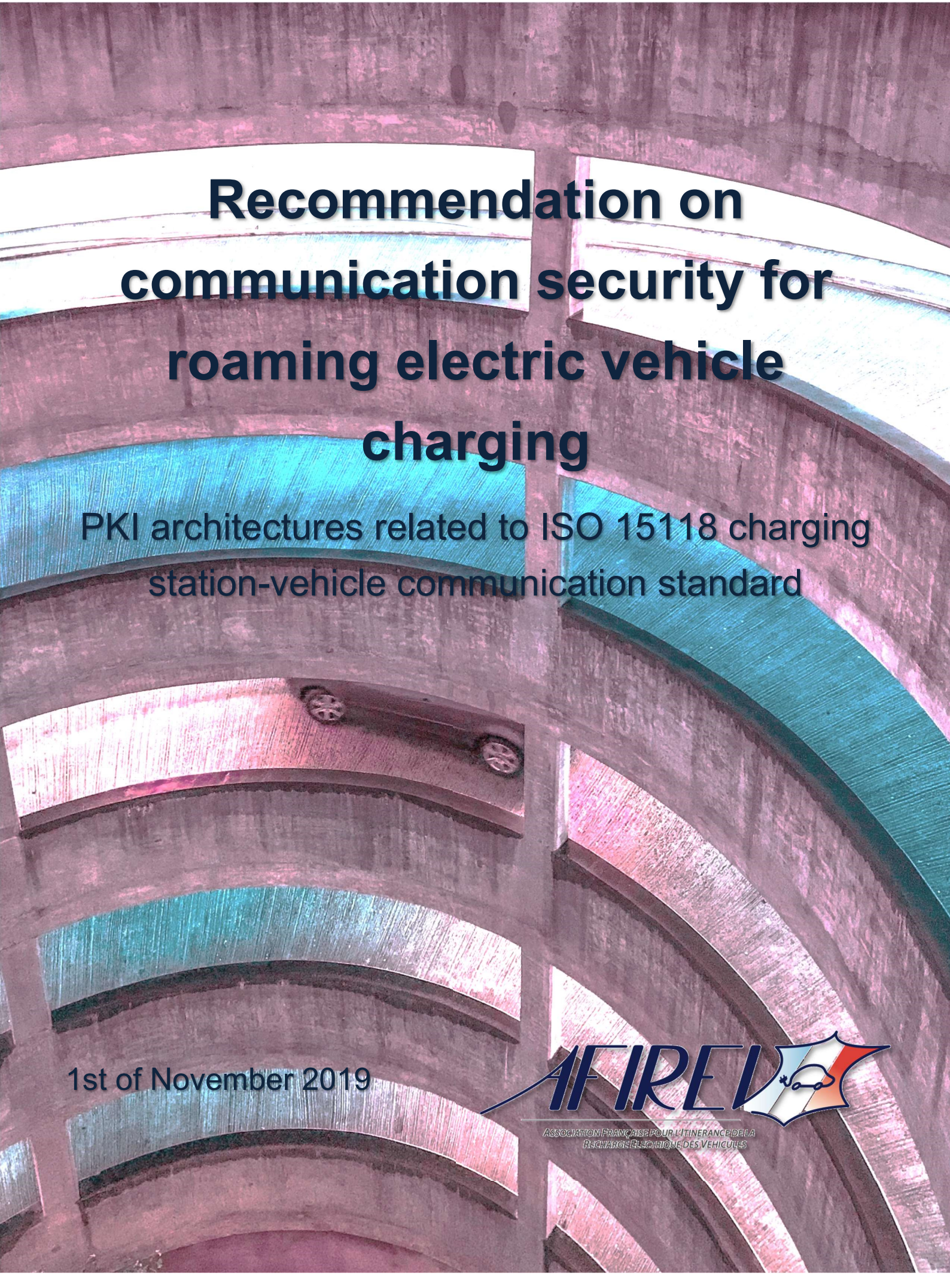

Recommendation on communication security for roaming electric vehicle charging

PKI architectures related to ISO 15118 charging station-vehicle communication standard

1st of November 2019

AFIREV
Association Française pour l'Itinérance de la Recharge Electrique des Vehicules

Table of content

Executive summary

The objective pursued by AFIREV in the context of this position paper on communication security for electric vehicle charging roaming is to build a French consensus on the implementation of a PKI architecture linked to the ISO 15118 communication standard. AFIREV wishes to propose a target architecture for the operation of the public key exchange infrastructure (PKI) allowing an open market in the management of these keys while guaranteeing a high level of security, reliability and ease of use as well as economic efficiency for the end customer. As part of this approach, AFIREV also wanted to address the organisation and management of *contract certificate pools* and the issue of loading these certificates into vehicles. The aim is to launch work at European Union level to prepare for maximum interoperability of functions proposed by ISO 15118.

AFIREV conducted an analysis of the strengths and weaknesses but also the opportunities, (SWOT) of the four possible architectures for the organization of the trust chain allowing certification (Root CA - Sub CAs - Certificate user):

- a unique and commercial certification authority
- a unique certification authority regulated at European or international level
- a federation of cross certifications between commercial certification authorities
- a bridge administrative authority allowing several regulated certification authorities

AFIREV assessed these architectures on the basis of transparency, interoperability, complexity and resilience.

In conclusion, AFIREV recommends a Multi-Regulated architecture based on a bridge administrative authority authorising several regulated certification authorities. It should be noted that this is the choice of the European Commission for Vehicle-to-Vehicle Communications (C-ITS). This architecture is a target to be achieved based on the current situation of coexistence of several Unique-Free architectures with commercial certification authorities and not necessarily interoperable. To ensure this transition, AFIREV has issued several recommendations to initiate discussions at the European level, in particular on the governance rules of this target architecture, including the subject of platforms, but also on the associated technical requirements.

AFIREV also studied the organisation for loading contract certificates into vehicles ensuring a level playing field for mobility operators and car manufacturers. A recommendation is made on this purpose concerning the structure of certificate trading platforms, its compatibility with the multi-regulated architecture and the management of these loadings (see Chapter 5).

AFIREV is now seeking the views and reflections of interested parties. Subsequently, AFIREV wishes to work through a collaborative project with the European electromobile industry to build a detailed consensus position on the governance of this PKI architecture. This position will be intended for the Directorate General for Mobility and Transport of the European Commission.

1. Introduction

The French Association for the Roaming of Electric Vehicle Recharging (AFIREV) was created at the initiative of the Minister of the Economy, Industry and Digital Technology at the Paris Motor Show in October 2014 and was officially launched in March 2015 by 7 major players in electric mobility: Bolloré BS, Bouygues Énergies Services, Engie Ineo, Gireve, Renault, Izivia (EDF Group), Vinci Energies. To date, they have been joined by the FNCCR, Freshmile, Easytrip, Chargemap, Spie, PSA, VEDECOM, Total EV charge, DKV France and IER, as well as interested third parties: École des Ponts Paristech, Solstyce, Schwartz & Co. Its purpose is to bring together initiatives that contribute to the deployment of the interoperability of charge and electric mobility services in France in order to create and maintain common elements between its players, represent their interests to regulatory authorities, ensure the international compatibility of solutions, and defend the French point of view versus European initiatives and bodies of the same nature.

This position paper sets out AFIREV's recommendations for the establishment of an organisation between stakeholders for the exchange of keys and certificates (PKI architecture) to secure the charging of electric vehicles using the ISO 15118 communication standard. These recommendations concern primarily France but with a vision of integration and interoperability in the European Union and on the European continent. This document focuses both on the architecture for generating certificates and security keys (*V2G Root CA* chain, *Sub-CA 1*, *Sub-CA 2*, Sn) and on making these elements available (*pool* management). It describes the main possible architectures based on the standard documents and the state of the art described by the electromobility industry:

- ISO 15118-1:2019 Road vehicles - Vehicle to grid communication interface - Part 1: General information and use-case definition
- ISO 15118-2:2014 Road vehicles - Vehicle-to-Grid Communication Interface - Part 2: Network and application protocol requirements
- “Exploring the Public Key Infrastructure for ISO 15118 in the EV charging ecosystem”, Elaad[1]
- “Handling of certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO 15118”, VDE[2]
- “Practical Considerations for Implementation and Scaling ISO 15118 into a Secure EV Charging Ecosystem”, ChargePoint, DigiCert, Eonti
- “Analysis of stakeholder views on key policy needs and options for action in Alternative Fuel Infrastructure deployment and consumer services”, Draft report from Sustainable Transport Forum
- “Secure and User-Friendly EV Charging, A Comparison of Autocharge and ISO 15118’s Plug & Charge” Hubject and V2G Clarity, July 2019

This document analyses the strengths and weaknesses inherent in each architecture as well as the opportunities and threats they may represent for the electromobility industry. Finally, this document makes a recommendation from the French industry for a PKI architecture and on the roadmap for its deployment in Europe and proposes a vision for structuring pools to complement the selected architectures.

[1] ElaadNL is a joint research centre for several Dutch grid operators in the field of intelligent charging infrastructures for electric vehicles.
[2] VDE is the "German Federation of Electrical, Electronic and Information Engineering Industries".

2. Terms and definitions

PKI Architecture: *Public Key Infrastructure* (PKI) Management Architecture, it is a public key infrastructure (PKI) management architecture. It is the architecture (organization, governance, procedures) to manage a set of physical components (computers, servers) and software designed to manage the public keys of a system's users, in this case the roaming electric vehicle charging system based on the ISO 15118 standard. *Source Wikipedia*[3]

Certificate: An electronic document that uses a digital signature to link a public key to an identity. Source *ISO 15118*

Public/private key: Public and private keys are used in asymmetric cryptography, there are two encryption keys, such that if the user uses a first key in a so-called "encryption" algorithm, the data becomes unintelligible to anyone who does not have the second key. The initial message can be found when this second key is given as the input of a so-called "decryption" algorithm. By convention, the decryption key is called the private key and the encryption key the public key. The key that is chosen private is never transmitted to anyone while the key that is chosen public is transferable without restrictions. *Source Wikipedia*[4]

Charge roaming: The ability for the user, whether or not he/she has a contract or subscription with a mobility operator, to use the charge networks of different recharging infrastructure operators without prior registration with the operator operating the network whose recharging service he/she occasionally uses, either by having access to the charge and payment for the service through a mobility operator with whom he/she has a contract or subscription, or by having access to the charge and payment for the service directly from the operator of the infrastructure to which he/she charges his/her vehicle. Source *French Decree No. 2017-26 of 12 January 2017*

***Leaf certificate*:** Any certificate that cannot be used to sign other certificates. For example: TLS / SSL client and server certificates, email certificates and any end-entity certificates. *Source Wikipedia*[5] This is the last level of certificate issued on the PKI chain. In the case discussed here, a mobility services contract certificate and a reload point certificate are *leaf certificates*.

Mobility Operator* (*eMSP) : *electro-Mobility Service Provider -*

- Entity with which a user contracts to have all EV-related services. *Source ISO 15118*
- Provider of mobility services for electric vehicle users including charge access services. *Source French Decree No. 2017-26 of 12 January 2017*

Charging Infrastructure Operator (CSO) : *Charging Service Operator -*

- Charging Infrastructure Operator - Actor responsible for the installation, O&M of charging infrastructure (including associated parking spaces) and power purchase management to meet energy demand at the charging point. *Source ISO 15118.* In fact, in the organization

[3] https://fr.wikipedia.org/wiki/Infrastructure_%C3%A0_cl%C3%A9s_publiques
[4] https://fr.wikipedia.org/wiki/Cryptographie_asym%C3%A9trique
[5] https://en.wikipedia.org/wiki/Public_key_certificate#End-entity_or_leaf_certificate

discussed here, the CSO is the actor who operates the recharging infrastructure to allow user access and ensure the recharging defined in its service.

- *A person who operates a recharging infrastructure on behalf of a developer or on their own account. Source French Decree No. 2017-26 of 12 January 2017*

Roaming operator (Interoperability Platform): an operator that contributes to the deployment of charge roaming by facilitating, securing and optimising data exchanges between charging infrastructure operators and mobility operators. *Source French Decree No. 2017-26 of 12 January 2017*

Pool: Entity where actors will deposit their public digital information in order to be able to associate the information quickly and easily.

Root certificate: root certificate - public key certificate that identifies a root certification authority - *Source Wikipedia*[6]

Sn : Physical element placed at the end of the PKI chain and having the leaf certificate. In this case, it is a vehicle, a charging point or a mobility services contract.

Sub CA**:** *Subaltern Certificate Authority, an* authority issuing a security certificate based on a root certificate of a PKI architecture for the charging service between electric vehicle and charging station. The ISO 15118 standard provides that 2 levels of *Sub-CA* are possible behind a *V2G Root CA*: the *V2G Root CA* certifies the *Sub-CA 1* which itself certifies the *Sub-CA 2*. The assignment of CA Subsidy roles is proposed in this document.

Trust List: The certificate trust list is a predefined list of items signed by the issuing entity of the certificate. It can be a list of names or files, all the elements it contains are authenticated and considered trustworthy by the issuing entity.

V2G root CA: *Vehicle-to-grid root Certificate Authority,* issuing the root security certificate of a PKI architecture for the charging service between electric vehicle and charging station. The V2G root CA and all actors who receive certificates from it and use them must be part of the same governance with its rules.

[6] https://fr.wikipedia.org/wiki/Certificat_racine

3. Element of context

3.1. This note responds to a problem presented by the sector

The implementation and management of PKI ISO 15118 architectures allowing secure exchanges and automatic authentication between vehicles, mobility contracts and charging infrastructures presents several issues to the industry that this document aims to address. These issues have been identified by the members of the sector represented within AFIREV and are based on the study of the state of the art presented in the introduction.

Market issues

Many players in the electromobility sector are convinced that its development is dependent on

- the level of openness of charging infrastructure networks,
- the establishment of transparent and fair market access conditions for both service and infrastructure operators,
- the ability of the sector to exchange real time information on the use of the charging infrastructure and services,
- alignment with common and interoperable communication standards and protocols.

Cybersecurity of communication around the recharging of electric vehicles is a transversal subject to these dependencies. The level of contribution of public actors and regulators to this cybersecurity workstream, particularly to remove certain barriers, is a subject discussed within the industry and is one of the elements addressed in this note.

The barriers to entry that could be posed by authentication mechanisms based on a PKI, such as the ISO 15118 standard discussed in this document, are sources of concern for some stakeholders. Through this document, AFIREV wishes to propose architecture and governance solutions that address these concerns.

The work carried out by AFIREV aims, among other things, to initiate discussions on PKI architectures that meet the expectations of the players in the sector by limiting monopolistic and oligopolistic positions. AFIREV's work is part of a charge roaming operation based mainly on *roaming* platforms.

AFIREV is convinced that the work to develop the PKI architecture complementing ISO 15118 is necessary because it does not exist and must be based on collective work by the industry on a European scale and not on the work of a small number of interested actors on a national scale that could lead to a deadly complexity for ISO 15118.

There is not yet a consensus on the entity or entities in charge of governance, implementation and management of the PKI architecture. On the other hand, many stakeholders seem convinced that the involvement of regulators would help to structure the ecosystem. The depth of this involvement still to be defined: governance, architecture definition, architecture management, etc.

The management of a *multi-root* PKI architecture or a unique *root* architecture is also a subject of debate that AFIREV wishes to clarify through this document.

Technical issues: IT and cybersecurity

It is obvious to the industry that the future of the charging infrastructures is to be connected and to offer multiple digital services. A robust (with identity certification, confidentiality and message integrity assurance) authentication management system that can support the growth of electric mobility therefore seems essential to many ecosystem stakeholders. The security and trust of charge point-vehicle communications is a pillar of recharging services because it is closely linked to payment mechanisms. Beyond interoperability on the user side, vehicles, EMSP..., this authentication management system must also be transparent towards a CPO's charging infrastructure assets and therefore interoperate with several charging infrastructure manufacturers.

The “Autocharge” technical solution is mentioned as an alternative to ISO 15118 with PKIs to perform the Plug and Charge function. This solution is based on the identification of the vehicle by the charging station through the (unique) MAC address of the vehicle's communication device. Like the ISO 15118 Plug and Charge, Autocharge provides a better charging user experience and better cybersecurity than with RFID cards (easily falsifiable).

Autocharge provides a higher level of security because it is more difficult to replicate a MAC address than an RFID badge, but it is not a secure identification method that would protect against interception of the user ID. Similarly, Autocharge does not allow you to manage compromised identifiers or encrypt the identifier. Although Autocharge is a simpler solution to implement, the fraud protection offered by this technical solution is considered insufficient compared to a communication protocol such as ISO 15118.

The industry seems convinced that the use of the ISO 15118 communication standard only guarantees a high level of security provided that it can be combined with a robust PKI architecture. The industry is also convinced that the "PKI" solution is the best.[7]

Concerns remain about certain technical aspects of the management of authentication certificates for mobility contracts, which some players in the sector consider too dependent on car manufacturers, with the risk of making their customers too captive.

It also seemed equally important for AFIREV to point out that CPOs have not yet8 been listed as "operators of essential services" in the EU, but that this future possibility should be considered in the reflection on architectures under construction in relation to cybersecurity.

[7] 89% positive response to the STF questionnaire (see Chapter 1. Introduction)
[8] European Directive (EU) 2016/1148

Points for improvement previously identified by the sector

Several stakeholders in the charge ecosystem point to the shortcomings of ISO 15118 (mainly its Part 2) in its ability to define a PKI architecture that provides enhanced, functional and scalable charge communication security.

AFIREV stresses that some of these aspects cannot be fully or partially covered by an ISO standard but are subject to organisational rules to be dealt with by the market and/or regulation. These elements are missing and make it difficult to deploy sufficient and easily scalable charge roaming communication security, but they must be defined by the industry in addition to ISO standards. The purpose of this document is to initiate some of these reflections.

In terms of governance, the lack of defined requirements for establishing the chain of trust, within or outside ISO 15118, as well as descriptions of certification processes and revocation of certification weaken security mechanisms and make it more complex to set up automatic authentication mechanisms.

Technical uncertainties such as the management of 2 or 3 levels of certification of your choice are also sources of weakness and complexity.

The remaining complexities, because they are not fully addressed, in the management of certificate life cycles and in the end-user's interaction with these certificates are also obstacles to be overcome in order to propose an architecture allowing secure vehicle charging infrastructure communication.

This recommendation document deals only with the chain of certifications and signatures guaranteeing the trust and security of exchanges between actors as well as the circulation of these certificates[9] for verification on platforms (*pools*). However, it does not address the IT and telecommunication architecture for the distribution, updating and revocation of certificates, in vehicles, charging infrastructures and information systems of the different stakeholders involved in the mobile charging of electric vehicles. It aims to propose recommendations to bring together stakeholders in the industry around a common position on the best solution for managing PKIs for the charge ecosystem in terms of governance, complexity, integration costs, cybersecurity, scale-up and interoperability.

3.2. PKI architectures studied

In this note, four possible PKI architectures have been analysed, based in particular on the Elaad[10]document. We have defined the following nomenclature

Unique indicates an architecture based on a unique V2G Root CA

Multi indicates an architecture based on several V2G Root CA

Regulated indicates an architecture with a regulatory authority

[9] The validity periods of the certificates will not be discussed in this document
[10] *"Exploring the Public Key Infrastructure for ISO 15118 in the EV charging ecosystem" – eLAAD*

Free indicates an architecture without a regulatory authority

The architectures studied are a combination of these criteria:

- ***Unique Free* Architecture (UF): A unique, market-based authority**

  In this architecture, the *V2G Root CA is a* commercial actor who is the sole manager of the certification system (in its governance and IT implementation) and who is responsible for its operation and interoperability. It therefore lays down the operating rules.

- ***Unique-Regulated* Architecture (UR): A unique authority regulated at European or international level**

  In this architecture, the *V2G Root CA* is a non-commercial actor regulated by a public authority (either a European regulatory authority or a consortium of private actors regulated by a European authority). This *V2G Root CA* can be divided into three parts:

  - Governance (we will call it *V2G Root CA* - "Regulatory Authority"): sets the rules of governance and applies them in an unambiguous way. He is the owner of the private key of the *V2G Root CA* and is responsible for the proper functioning of the certification system.
  - Certification operation (we will call it *V2G Root CA* - "Certification System Manager"): selected following a call for tenders issued by the *V2G Root CA* - "Regulatory Authority". He manages the IT system. He uses the private key during certification but is not necessarily aware of it. By complying with the standards in force (ISO 27001, etc.) and the additional requirements of the regulatory authority.
  - Audit (we will call it *V2G Root CA* - "Auditor"): selected following a call for tenders issued by *V2G Root CA* - "Regulatory Authority", it audits the *V2G Root CA* - "Certification System Manager" (audit to be made public).

- ***Multi-Free* Architecture (MF): A federation of cross certifications**

  In this architecture, there is not one but several *V2G Root CAs* that coexist and whose legal structure is not imposed. Each *V2G Root CA* manages its own certification chain in a way comparable to UF or UR architectures. In order to ensure system interoperability, a bilateral link between *V2G Root CAs* is necessary. Each *V2G Root CA* creates and maintains its own *trust list*[11] integrating all established trust links. The *trusts lists* are thus unique to a *V2G Root CA* and independent of each other.

- ***Multi-Regulated* Architecture (MR): A bridge administrative authority**

  As in the MF architecture, there is not one but several *V2G Root CAs* that coexist and whose legal structure is not imposed. Each *V2G Root CA* manages its own certification chain in a way comparable to UF or UR architectures. However, unlike the *Multi-Libre* architecture, system interoperability is managed by an administrative authority whose mission is to create a unique *trust list*, maintain it and transmit it to all *V2G Root CAs* on this list. This authority sets minimum governance rules that must be respected by any new

[11] The mechanism for managing *trust lists* is not specified in ISO 15118. The process of transferring, securing, updating and decrypting *trust lists* remains to be defined for PnC if the C and/or D architectures are selected.

V2G Root CA wishing to join the *trust list* to be interoperable. In order to verify compliance with these minimum governance rules, the administrative authority publishes specifications and calls upon a specialised audit firm to audit new applicants and monitor the listed members.

It is important to remember that it is still possible for any actor to set up an independent PKI architecture to manage the security of exchanges in an electric vehicle charging service, and therefore any economic actor remains free to set up *V2G root CA*. On the other hand, the coexistence of multiple PKI management architectures is a major obstacle to the interoperability of charging services and therefore to the roaming. In France a public charging infrastructure that would be linked to such an independent PKI architecture would therefore not comply with Article 12 of Decree No. 2017-26 of 12 January 2017.

An additional cybersecurity issue needs to be considered. By definition, the implementation of a PKI architecture makes it possible to secure certificate exchanges. Any cyber-attack on the system will necessarily lead to serious malfunctions that may lead to the suspension of the Plug'n' Charge functionality for an indefinite period of time. The objective of this document is not to give technical recommendations on the cybersecurity of the IT system but it seems appropriate to estimate the impact of a system compromise on the PKI architectures considered in order to raise some points of attention.

As an example, and to illustrate each of the document's architectures, we will consider the following example:

- ***V2G Root CA*:** One or more root certificate certification authority(ies) depending on the architecture, the number will be specified in the description of each architecture,
- ***Sub-CA 1*:** A Europe-wide charging infrastructure operator (*CSO*),
- ***Sub-CA 2*:** A French subsidiary of this *CSO* operating exclusively on expressways and motorways
- **S1 to Sn:** A fleet of n bollards on expressways and motorways in France managed by this *CSO*,
- **An electric vehicle** with a mobility contract signed by the or one of the *V2G Root CAs.*

3.3. Method used for the evaluation of PKI architectures

The architectures will be evaluated on 2 axes[12]:

- Advantages and disadvantages of this architecture for the roaming electric vehicle charging industry: **OPPORTUNITY** or **Threat**
- Advantages and disadvantages of this architecture for the actor or actors operating and governing the V2G root CA: **STRENGTH** or **WEAKNESS**

and on 10 criteria:

[12] SWOT methodology

Critère 1. Transparency of the *V2G Root CA*:

This criterion makes it possible to assess the accessibility of *V2G Root CA-dependent* players to information relating to governance, pricing grids, contractual terms and conditions and rules for managing *V2G Root CA* services (SLA, support, etc.). It also considers the involvement of these actors by the *V2G Root CA in the* definition and drafting of governance rules and other criteria that impact them.

Critère 2. Distribution of *V2G Root CA* functions :

In the operation of the PKI architecture, the *V2G Root CA* plays a central role and provides three main functions that can be distributed among several actors:

- Governance" function: The *V2G Root CA* - "Governance Authority" is responsible for defining the specifications to be respected for any new Sub-CA 1 wishing to be certified, holds the private key of the *V2G Root CA* and guarantees the proper functioning of the PKI architecture. The actor in charge of governance can issue calls for tenders and subcontract the following two functions.
- Certification Operation Function: The *V2G Root CA* - "Certification System Manager" is responsible for operating the IT system to certify the actors. He can use the private key for certification but without necessarily being aware of it.
- "Audit" function: The *V2G Root CA* - "Auditor" is responsible for auditing at the technical, political and financial level the actor performing the "certification operation" function and any actor wishing to be certified according to specifications defined by the governance entity.

Critère 3. System interoperability:

Interoperability is based on the ability of systems to exchange information and to work together seamlessly. This criterion makes it possible to analyse the impact of the implementation of the PKI architecture in question on the functioning of the interoperability of the charge roaming system. It also considers the opening of the architecture[13] to other markets, such as non-European markets.

Critère 4. Complexity of implementation and deployment:

The deployment of architectures is not so much on a technical level (IT developments, complexity of processes, definition of new methods), on a political level (acceptability by stakeholders, need to regulate) or on a temporal level (time required for implementation, time required for implementation of the architecture, time required for decision-making). This criterion will make it possible to assess the rest to be done for each PKI architecture considered.

Critère 5. Existence of barriers to entry to be *V2G Root CA*:

In accordance with competition and anti-trust rules, any new player is able to declare itself V2G Root CA. Using this criterion, we will analyse the brakes introduced by each architecture for the creation of new *V2G Root CAs*.

Critère 6. Scalability of the system:

[13] The ISO 15118 standard recommends the installation of 5 *V2G Root CAs* worldwide (1 per continent) and the installation of 5 *V2G Root CA Certificates* in each electric vehicle

Each certificate has its own life cycle, which may differ depending on the PKI architecture chosen. It is therefore necessary to assess the system's ability to evolve in a secure way, i.e. accept replacements or updates of certificates while ensuring the security (physical and cyber) of processes.

Critère 7. Economic and technical resilience of the *V2G Root CA*:

The resilience of a system is its ability to overcome rare and disruptive events without impacting its level of functioning. For each PKI architecture, we will evaluate the resilience of the *V2G Root CA* against:

- An economically disruptive event: bankruptcy of V2G Root CA, takeover of V2G Root CA by another company,
- A disruptive event of a technical nature: failure of the certification system, compromise of the V2G Root CA, cyber-attack.

In accordance with ISO 15118, a *V2G Root CA* cannot generate a *Leaf Certificate*, so it is necessary to have a PKI architecture with at least 3 depth levels (Root CA, Sub CA, Sn). This depth is also limited to 4 by ISO 15118. All the architectures considered allow for a maximum structure in terms of depth level. This criterion will therefore not be discriminatory, and is therefore deliberately excluded in the evaluation of architectures.

4. Synthesis of the analysis and choice of the PKI architecture

4.1. Four prioritized selection criteria

The analysis of the 4 architectures carried out according to the seven predefined criteria made it possible to draw conclusions on a choice of target PKI architecture based on the prioritisation of certain criteria. AFIREV has prioritised the four most discriminating criteria, the other three criteria allow a better understanding of the issues at stake in each architecture and have been considered when drawing conclusions.

The prioritized selection criteria are listed below:

- **Criterion 1: Transparency of the *V2G Root CA*:**

  The PKI architecture to be implemented must encourage transparency of the *V2G Root CAs* both in the establishment of governance rules and in the choice of tariffs and tariff rules. The transparency of the *V2G Root CAs* would ensure a stable and non-discriminatory certification system.

- **Criterion 3: Interoperability of the system:**

  System interoperability is based on technical cooperation of IT systems and is a basis for providing customers with a seamless experience of the PnC charging function. The PKI architecture chosen should ensure a reliable, simple and secure roaming service over the widest possible geographical area.

- **Criterion 4: Complexity of implementation and deployment:**

  The architecture chosen should allow a good compromise between:

  - an easy implementation of the technical solution allowing a simple operation of the architecture and certification system,
  - effective decision-making with the definition of governance rules that are appropriate for stakeholders,
  - rapid implementation and deployment, with technical developments and decisions that can be made within a reasonable time.

- **Criterion 7. Economic and technical resilience of the *V2G Root CA*:**

  The architecture chosen must be economically and technically resilient in order to ensure the sustainability of the architecture and the security of certificate exchanges. The choice of AFIREV will also be motivated by an intrinsic capacity of the architecture to encourage permanent innovation of the processes put in place as well as to ensure continuous supervision of the existing ones.

4.2. Choice of architecture

The AFIREV study thus favours MR architecture based on a bridge administrative authority authorising several regulated certification authorities.

A *Regulated* architecture can be seen as a unifying architecture. The advantage of delegating governance to a public entity or a private but regulated consortium is full transparency of governance rules and tariffs, an interoperable, resilient and resilient system with simple implementation. Indeed, the competition of *V2G Root CAs* - "Certification System Manager" via calls for tenders will encourage innovation while reducing certification fees. The shorter the time between each call for tenders, the greater the incentives for innovation. In addition, this system for separating the functions of the *V2G Root CA makes it* possible to have a resilient architecture both economically (the *V2G Root CA* - "Governance Authority" has a very low probability of bankruptcy; the *V2G Root CA* - "Certification System Manager" and the *V2G Root CA* - "Auditor" can be replaced at any time) and technically by defining precise specifications during the tender process and monitoring its compliance over time by all stakeholders.

However, the establishment of a European regulatory authority may take time. The time required for decision-making can be quite long because several actors will have to agree. This could affect the simplicity of operation of this system. In addition, combined with reasons of system security and stability, delays between calls for tenders are likely to be high, which would probably lead to IT systems that are increasingly uncorrelated to the market. In addition to these obstacles, there is the risk of a conflict of interest: in the event of governance by a regulated private consortium, can a member of the consortium manage the certification system?

The *Multi-Regulated* architecture encourages the coexistence of several *V2G Root CAs* and therefore to have a more competitive system. As a result, this PKI architecture further encourages certification system managers to innovate and offer increasingly secure systems while reducing their costs. The administrative authority would guarantee a minimum transparency of any *V2G Root CA* wishing to be interoperable. By respecting minimum governance rules (RGM), all *V2G Root CAs* registered on the unique *trust list* are committed to providing a viable roaming service. As for decision times, they are reduced due to the autonomous management of each architecture by its *V2G Root CA*. On the other hand, the existence of an administrative authority in charge of managing the *trust list*, and therefore of interoperability, makes it possible to have a resilient system (economically and technically), non-discriminatory and open to any new entrant as soon as it respects the RGMs.

Although the MR architecture may seem to be the reference solution for the deployment of a PKI architecture, it still faces a major technical complexity: the management of the *trust list*. *Trust list* technology is commonly used in IT systems that can exchange information without interruption and without file size limits, such as C-ITS (Chapter 8). However, this technology is not defined in ISO 15118. However, in this architecture, roaming is expressly dependent on the management of this *trust list*. A major challenge is therefore the definition of specifications common to the entire industry for the implementation of mechanisms for setting up a trust list, processes for securing the list, protocols for transferring and updating this list as well as secure decryption algorithms. The implementation of an MR-type architecture is therefore constrained by potentially long

decision-making, technical development and integration times. A more detailed analysis of the technical solutions that can be considered for a *trust list* or as a replacement for a *trust list*, as well as the deadlines for drafting specifications applicable to the entire sector and for setting up the *trust list* management mechanism, should be carried out.

Trust list management in MR architecture introduces a technical barrier at the entrance for bollards or vehicles designed for markets operating with *V2G root CAs* without *trust list* (UF or UR architecture). Indeed, it is necessary that charging infrastructures and vehicles are able to handle this *trust list* (coding, decoding, interpretation, updating, revocation...), a software update will therefore be necessary in addition to updating the certificates to use them on a European plate with a PKI architecture of the MR type.

Thus, feasibility pitfalls remain to be resolved for the implementation of a MR-type architecture in both areas: governance and technical management. In particular, a balance will have to be found between speed of implementation, openness and security of the architecture. The adoption of a regulated architecture is based first of all on the appointment of a federating governance entity (public or a consortium of actors) in charge of publishing governance and audit rules in order to authenticate the actors wishing to integrate the PKI architecture.

The transition to a *Multi-Regulated* architecture. In the event that the *Multi-Regulated* architecture is adopted, and as reservations still persist for the implementation of this architecture in the terms defined in section 7.4, it would be preferable to consider a transitional phase limiting the action of the administrative authority to governance and the publication of rules common to the sector. As the current situation is moving towards a coexistence of non-interoperable UF architectures in this first phase, governance could be managed by a consortium of regulated actors or with the endorsement of regulatory actors and would rely on existing technical actors to ensure the interoperability of systems. In view of the small number of Root CAs planned, the use of *trust lists does not* seem necessary to date. Indeed, simple and temporary solutions can be considered such as the installation of several *root certificates* in charging infrastructures and vehicles. Thus, initially, this authority will only be responsible for defining the minimum common governance rules to be respected by *V2G Root CAs* while having the power to monitor compliance with these rules. In parallel, work will have to be done to define and draft the rules for managing the *trust list*. Once the architecture is anchored and the *trust list* management mechanisms are in place, the administrative authority will become more operational and will be in charge of managing the unique *trust list of* the PKI architecture. This second phase will further open the market to new *V2G Root CAs*. This two-step implementation will save significant time for the deployment of the MR type architecture while ensuring compliance with the criteria defined by AFIREV.

Concerning the UF and MF architectures, they have not been selected as targets for the following reasons:

- *The Unique Free* architecture, although the simplest and fastest to implement, has many drawbacks and risks to the transparency, interoperability and resilience of the system. Being neither regulated, nor competitive, nor audited by an independent actor, the *V2G Root CA* will have control over the entire certification operating system and will carry all

financial, cyber security and other risks. This architecture therefore does not meet the AFIREV criteria.

- Concerning the *Multi-Free* architecture, the introduction of competition will allow a stable and more resilient system with potentially more transparent *V2G Root CAs.* Interoperability will therefore no longer be based on a unique actor but will be spread over a number of N *V2G Root CAs*. However, the implementation of this system is based on the implementation of bilateral agreements and the use of N *trust lists* (unique by *V2G Root CA*). The time required to define common rules for the creation and management of *trust lists*, the development times still unknown for the implementation of this mechanism and above all the discriminatory aspect made possible by the absence of regulation are all risks that lead AFIREV to reject this architecture.

5. Summary of the analysis on the structuring of certificate trading platforms

5.1. Use cases of pool platforms

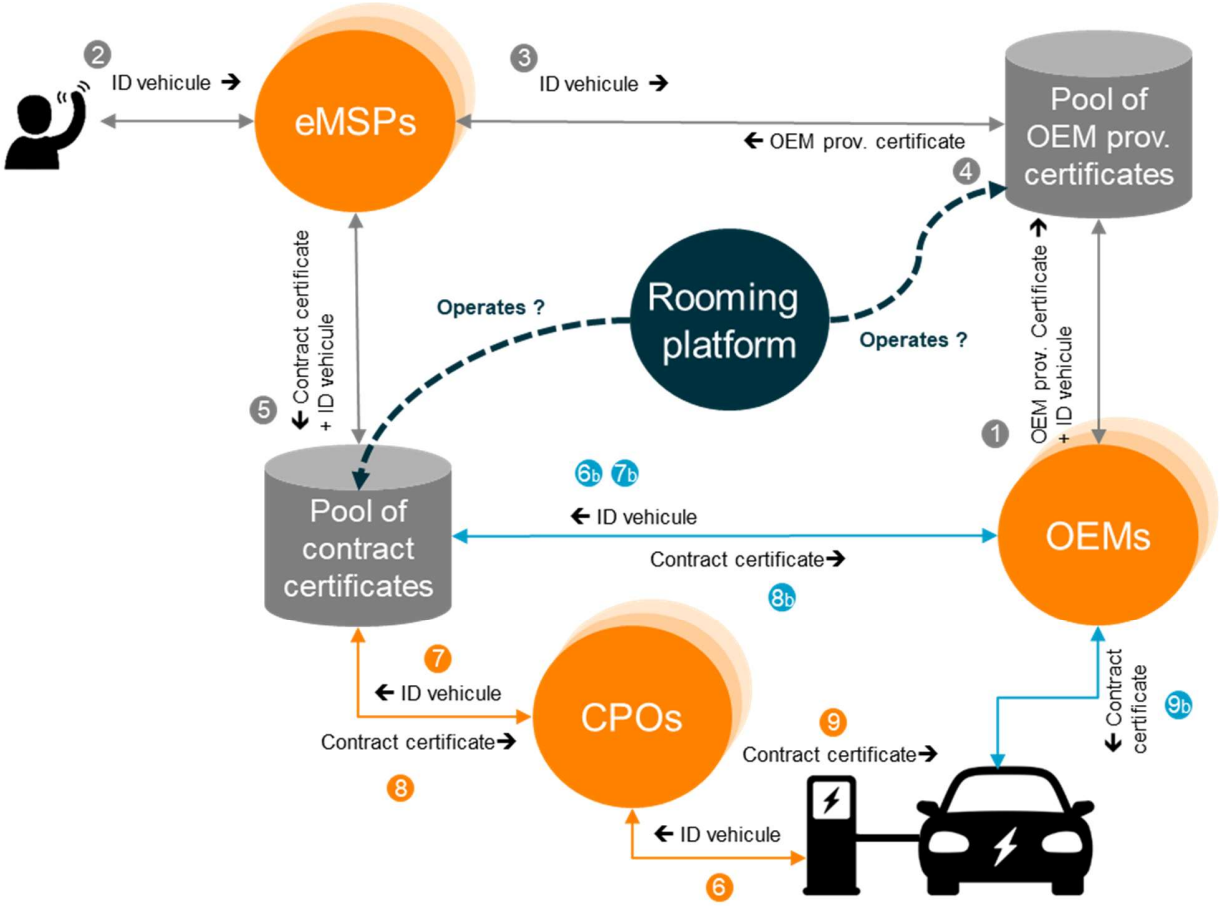

Figure 1 - Operating diagram of the pools associated with the management of contract certificates

In the context of ISO 15118 and the Plug and Charge function, certificate exchange platforms are used for 3 major use cases: the installation of a mobility contract certificate in a vehicle, the revocation of this contract certificate, and the replacement of one contract certificate by another. We present the functioning of these platforms in a simplified way in order to discuss the possible impacts of the reflections on PKI architectures on these platforms.

The installation of a mobility contract certificate follows the following steps:

1. Before the vehicle is handed over to its owner, the car manufacturer deposits on an exchange platform the *OEM provisioning certificate* associated with the vehicle ID (vehicle ID)
2. The vehicle user contracts with a mobility operator (eMSP) by providing him with his vehicle ID, among other things

3. From this vehicle ID the eMSP requests the *OEM provisioning* certificates exchange platform to obtain the certificate corresponding to the new customer's vehicle.
4. The *Pool of OEM provisioning certificate* provides the corresponding certificate and thus the eMSP can create a *Contract certificate from the contract* information (expiry date, etc.), containing its vehicle ID and sign it with the OEM provisioning certificate specifically for its customer's vehicle
5. The eMSP deposits on an exchange platform the contract *certificate* associated with the vehicle identifier (vehicle ID)

There are then several methods to install this certificate we present two of them

6	During a first connection to an ISO 15118 charging infrastructure, the absence of a *contract certificate* in the vehicle leads to the charging infrastructure requesting its CPO to obtain one for the vehicle, for this purpose it provides it with the vehicle ID	6b - 8b	The *Pool of contract certificates* provides the OEM with the *contract certificates* corresponding to the vehicles of its manufacture from their run-of-river vehicle IDs and/or on request
7	With the vehicle ID the CPO requests the *Pool of contract certificates*		
8	The *Pool of contract certificates* provides the CPO with the *contract certificate* corresponding to the vehicle if it exists		
9	The *contract certificate* corresponding to the vehicle is lowered to the vehicle, via the bollard, to be installed there	9b	The OEM installs via a telematic link the *contract certificate* requested by its customer

Other installation methods may be considered such as manual updating via a physical or non-physical medium of the vehicle by its owner or a professional.

The revocation of a contract certificate leads an eMSP to update the *Pool of contract certificate,* it must also be managed within the vehicle so that a contract certificate identified as revoked is not stored unnecessarily (uninstallation, overwriting by another certificate, etc.).

5.2. Compatibility of certificate circulation with the selected UR and MR architectures

There is no impact of the choice of PKI architecture on the structuring of pools and their management. Whatever the architecture chosen, it is necessary to set up two pools to be able to manage the use cases of creation of the mobility contract certificate (contract certificate), its installation and its revocation.

The management, governance and market rules related to the establishment of these pools and the coexistence of several pool managers and therefore several pools for contract certificates and several pools for *OEM provisioning certificates* are subjects that, as for the PKI management architecture, remain to be defined.

For AFIREV it is important to lead discussions and consensus building at the European continental plate level via the EU on the subject of ISO 15118 PKI architectures and ISO 15118 certificate pools, particularly on governance management.

5.3. Management of certificate loading in EVs

The installation of a mobility contract certificate in the electric vehicle equipped with ISO 15118 Plug and Charge technology is a key step in enabling this advanced charging service. Several installation channels are possible (manual, via the charging infrastructure, in dealership, via telematics), and it seems that a consensus is emerging among car manufacturers to set up an installation process via the telematics link (telecommunication link, 3G, 4G...) between the vehicle and a management server on the manufacturer side.

For car manufacturers, this channel is the most transparent for the user experience because it allows digitalized and simplified certificate management, outside the recharging process, for example following contractualization with an eMSP. This channel also allows for the management of multiple mobility contracts and greatly facilitates the change of eMSP (installation of a new contract certificate), the termination of a contract (revocation of the certificate) and the alternation between several contracts - professional and personal for example (exchange of certificates).

Automobile manufacturers therefore want to be connected to the contract certificate pool manager to immediately offer the customer the update of the contract in his vehicle as soon as a new certificate is available for his vehicle in the pool (push mode).

This solution seems to be at the service of the user experience while allowing free competition from eMSPs on the Plug and Charge ISO 15118 recharging service, it must nevertheless be completed to provide all the guarantees to the players in the industry on free and fair access to the installation of contract certificates in vehicles.

6. AFIREV Recommendations

AFIREV work carried out on the PKI architectures to be deployed primarily in France but with a vision of integration and interoperability in the European Union and on the European continent has led to the following recommendations:

> **Recommendation 1:** AFIREV recommends initiating Europe-wide discussions with the aim of building consensus by targeting the following PKI architecture: *Multi-Regulated* Architecture based on a bridge administrative authority

For the implementation of a UR or MR type architecture, common governance rules must be established.

Considering that:

- Stakeholders have taken initiatives that are in line with MR architecture;
- The MR architecture must be defined in consultation with the European authorities, which could take an indefinite period of time;
- Convergence with the C-ITS organization must be planned in the long term;
- It seems that the European Commission has chosen the MR architecture for C-ITS (see 8. Annex);

It seems preferable to start with the implementation of common governance rules from the perspective of an organization in MR architecture.

> **Recommendation 2:** AFIREV recommends the emergence of a project management system for the *Multi-Regulated* architecture managed by a group of stakeholders or a public entity, for the definition of minimum governance rules common to the entire supply chain and having the power to control the monitoring of these rules. This entity is not necessarily linked to the European Union in the first instance but will have to federate on a continental scale in the medium term. This project must be collaborative in order to bring together the multiple actors and consortia that have taken a position on the subject of PKI for ISO 15118 and wish to see this subject succeed. It will have to rely on technical expertise on the subject of PKI management.

The governance rules of the two architectures are complex elements to define but also key to federate the sector around an architecture

> **Recommendation 3:** AFIREV recommends the development of European-wide governance rules for the preferred PKI architecture (*Multi-Regulated*) that cover platform topics (pool), rules for certification and audit of *Sub-CA* candidates and minimum requirements for actors operating certification systems.

The technical management of *trust lists* is a major challenge for the implementation of the MR architecture

> **Recommendation 4:** AFIREV recommends that the industry study at European level of technical specifications and governance rules for *trust list* management or alternative technical solutions (specifications common to the entire industry for the implementation of mechanisms for setting up a trust list, processes for securing the list, transfer protocols and updating this list as well as secure decryption algorithms).

The management of certificate circulation platforms (pools) and the loading of certificates into vehicles are also challenges for the development of ISO 15118's advanced services such as Plug and Charge and their cybersecurity.

> **Recommendation 5:** AFIREV recommends that discussions be held with the aim of reaching a consensus at the European continental plate level via the EU on the subject of ISO 15118 certificate pools, in particular on the management of their governance and on the process of loading certificates into vehicles guaranteeing free and fair access for all EMSPs

7. Appendix - Description of architectures and evaluation

7.1. UF Architecture: A unique and marketable authority

7.1.1. Description

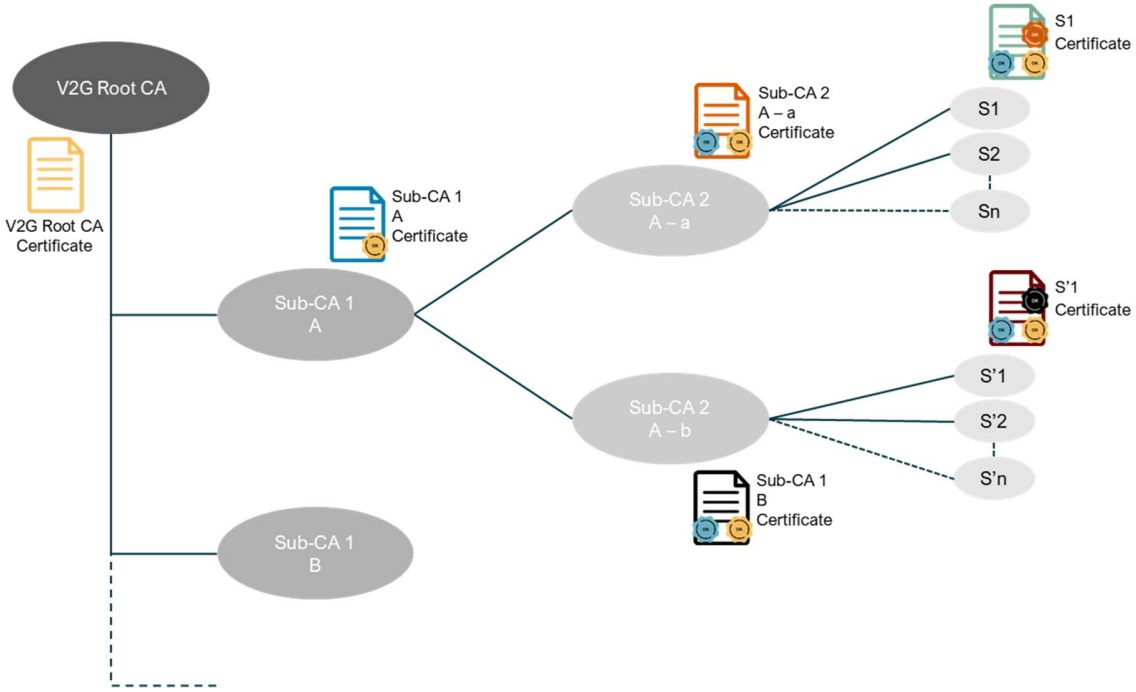

Figure 2 - Block diagram of the UF architecture "A unique and commercial authority".

The *V2G Root CA* is an economic, commercial and unregulated player. In this architecture, it is the only authority that can issue root certificates (*V2G Root CA Certificates*) and therefore certify the actors associated with it and thus allow the security of the PKI architecture. Any actor with the *V2G Root CA* certificate in their certificate chain or signatures is considered a "trusted actor" on all authentication chains. The V2G Root CA carries out audits of *Sub CA* candidates and the management of certificates by the actors who request it.

As an illustration, let us consider the example defined at the beginning. In this architecture, the *V2G Root CA* sets governance rules and fees for any *CSO* wishing to be certified. The European *CSO* requests to be certified for a fee, thus granting it the right to generate *Sub CA Certificates* signed by the *V2G root CA*. This *CSO* certifies its French subsidiary for motorways by issuing a certificate containing the signature of the *V2G Root CA*. In this way, the subsidiary is certified as a trusted actor and is authorized to generate and install *leaf certificates* in the charging

infrastructure park it operates. These certificates in the charging infrastructures also contain the signature of the *V2G Root CA*, ensuring a trustworthy link for the vehicles that connect to it.

After connecting the electric vehicle to the charging infrastructure, the latter sends its *Contract Certificate*. The charging infrastructure checks that the *V2G Root CA* has signed the vehicle's mobility certificate and that it corresponds to the one that signed its *leaf certificate*. In the event of success, a bond of trust is therefore established between the two.

7.1.2. UF Architecture Evaluation Criteria

Criteria	Evaluation on both axes (internal and sector)
Number of V2G Root CA	1
Legal structure of the *V2G Root CA*	Unregulated private company
1. Transparency of the *V2G Root CA*	**Threat:** The V2G Root CA sets the rules of governance and applies them to all its customers, it can change them at its discretion. It is only bound by the General Trade and Competition Codes. **Threat:** The V2G Root CA decides its rates and level of service, it can modify them at its discretion. It is bound only by its signed contracts and the General Commercial and Competition Codes. **WEAKNESS:** The existence of a unique private *V2G Root CA* is not compatible with European competition and antitrust rules.
2. Distribution of the functions of the *V2G Root CA*	**STRENGTH:** The *V2G Root CA* operates the only **IT** system that generates *V2G Root CA* Certificates and establishes governance rules. Consistency and speed of execution are therefore expected. **Threat:** All players depend on the same *V2G Root CA* and its IT system. They have no right of access. **Threat:** No audit of the *V2G root CA* is possible a priori.
3. System interoperability	**STRENGTH:** The interoperability system is based solely on the *V2G Root CA*, and its ability to generate certificates. Managing interoperability is therefore simple. **OPPORTUNITY:** In the event of a geographical change of a vehicle from one *V2G Root CA* operating plate to another (e. g. resale or import of a vehicle outside Europe), it is sufficient to install the new *V2G Root CA Certificate* in the vehicle to ensure interoperability. **Threat:** In the event of a *Sub-CA* disagreement, with the *V2G Root CA*, the third-party system is not or no longer

	interoperable with the rest of the systems contracted with the *V2G Root CA*. **Threat:** The monopolistic position of the *V2G Root CA* could lead to a high discriminatory potential, which would lead to a fragility of the system.
4. Complexity of implementation and deployment	**STRENGTH:** Simple implementation due to the uniqueness of the solution and its management by a unique actor and decision-maker, it is the simplest and certainly the fastest architecture to deploy. **STRENGTH:** Simple management of governance rules due to the uniqueness of the decision-maker. **Threat:** Governance rules, tariffs and technical solutions may change without notice and without the right of third parties to control, so complexity may be transferred to *Sub-CAs*.
5. Existence of barriers to entry to be *V2G Root CA*	**OPPORTUNITY:** No additional regulatory or technical barriers to entry to become *V2G root CA* **Threat:** This architecture promotes the existence of a monopoly, discouraging the creation of new *V2G Root CAs*.
6. Scalability of the system	**STRENGTH:** The uniqueness of the *V2G Root CA Certificate* allows you to limit the number of updates, renewals or replacements of this certificate. **Threat:** The uniqueness of the V2G Root CA and the IT system hinders creativity and initiative in improving and securing implemented processes.
7. Economic and technical resilience of the *V2G Root CA*	**WEAKNESS:** In the event of bankruptcy, no more recharging is possible on charging infrastructures with a *Leaf Certificate* signed with this *V2G Root CA*. **Threat:** *V2G Root CA* may go bankrupt or be acquired by a third-party company potentially leading to drastic changes in the governance rules and tariffs applied without the right of scrutiny of the actor's dependent on *V2G Root CA*. **Threat:** The breach of the *V2G root CA* is aggravated by its non-transparent governance (communication rules on self-defined security vulnerabilities, limited auditability, etc.) **Threat:** A cyber-attack on the certification system would cause heavy technical (restricted or blocked operation of the system, non-security of exchanges in the event of non-communication of the system's compromise) and financial (significant investments in cybersecurity to compensate for the defect and penalties) impacts. This could lead to the bankruptcy or takeover of the *V2G Root CA*.

	STRENGTH: Rapid decision making in terms of cybersecurity due to the fact that the *V2G Root CA* is a centralized player.

7.2. UR Architecture: A unique authority regulated at European or international level

7.2.1. Description

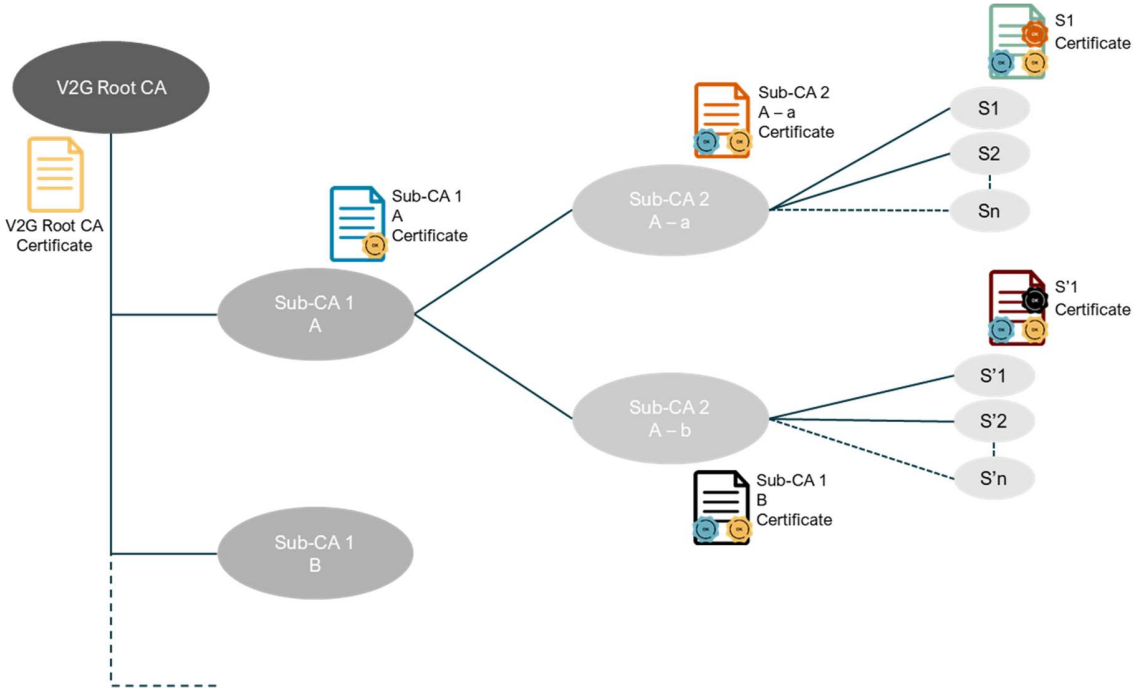

Figure 3 - Block diagram of the UR architecture "A unique authority regulated at European or international level"

The *V2G Root CA* is *a* neutral, regulated and non-market player. It is managed by a European or international entity - which we will call a regulatory authority - or by a consortium of private actors regulated by a European or international body that ensures the implementation of non-discriminatory rules for membership of the consortium - we will call it a regulated consortium. This *V2G Root CA* (regulatory authority or regulated consortium) guarantees the proper functioning of the architecture and transparency of governance rules and pricing rules. This *V2G Root CA* is considered by the entire industry as the only authority that can issue root certificates (*V2G Root CA Certificates*) and therefore certify the actors associated with it and thus allow the security of the PKI architecture. Any actor with the *V2G Root CA Certificate* is considered a "trusted actor" on all authentication chains.

This *V2G Root CA* can be a purely administrative authority without the technical skills required to manage the certification and outsource the management of the IT system for signing certificates and auditing the actors to be certified (*Sub-CA 1*) to third party actors through calls for tenders. All respondents may, during the selection process of the service provider, be audited by an independent entity and mandated by the regulatory authority. To summarize, three functions appear:

- Definition of governance and tariff rules: managed by the governance authority (regulatory authority or regulated consortium) which sets clearly established and shared governance rules. As for the tariffs, they can be defined a priori or posteriori for calls for tenders; they nevertheless remain fixed and known by all the actors concerned in the chain,
- Management of the certification system: managed by the governance authority if it has the necessary skills or by an external service provider after a call for tenders. In the second case, the service provider is responsible for maintaining the system in operational condition while the governance authority is responsible for the proper functioning of the certification chain,
- Audit of *Sub-CA* candidates and certificate management: managed by the governance authority if it has the necessary skills or entrusted to an independent specialised body in charge of verifying the ability of the respondent to operate the certification system. The audit of the *V2G Root CA* - "Certification System Manager" can be made public for the sake of transparency.

As an illustration, we will consider the example defined at the beginning. In this architecture, the *V2G Root CA* - "Governance Authority" sets governance rules, defines the tariffs and makes them available to any *CSO* wishing to be certified. Following two calls for tenders, it selects a *V2G Root CA* - "Auditor" and a *V2G Root CA* - "Certification System Manager" which it regularly audit in order to ensure a good level of service.

The European *CSO* is applying for certification. After an audit by the *V2G Root CA* - "Auditor", the *V2G Root CA* - "Certification System Manager" certifies the *CSO* thus granting it the right to generate *Sub CA Certificates* signed by the *V2G root CA*. This *CSO* certifies its French subsidiary for motorways by issuing a certificate containing the signature of the *V2G Root CA*. In this way, the subsidiary is certified as a trusted actor and is authorized to generate and install *leaf certificates* in the infrastructure it operates. These certificates in the charging infrastructures also contain the signature of the *V2G Root CA*, ensuring a trustworthy link for the vehicles that connect to it.

After connecting the electric vehicle to the charging infrastructure, the latter sends its *Contract Certificate*. The charging infrastructure checks that the *V2G Root CA* has signed the vehicle's mobility certificate and that it corresponds to the one that signed its *leaf certificate*. In the event of success, a bond of trust is therefore established between the two.

7.2.2. Criteria for evaluating the UR architecture

Criteria	Evaluation on both axes (internal and sector)
Number of *V2G Root CA*	1
Legal structure of the *V2G Root CA*	Neutral and regulated entity (company, association, organization)
1. Transparency of the *V2G Root CA*	**STRENGTH:** Governance rules are established and evolve through regulation and are therefore known to all. The actors depending on the *V2G root CA* are aware of these rules and can even contribute to their implementation or evaluation. **STRENGTH:** The certification rate of the *V2G Root CA* is regulated and known by the various players.
2. Distribution of the functions of the *V2G Root CA*	**STRENGTH:** A separation can be set up between the different functions of the *V2G Root CA*: • Governance by an independent authority • Operational management of certificate generation managed by a third-party IT actor • Audit of the actors (IT system manager and Sub-CA 1) by a specialized actor
3. System interoperability	**STRENGTH:** The interoperability system is based solely on the *V2G Root CA*, and its ability to generate certificates **STRENGTH:** The existence of a non-market administrative authority makes it possible to federate the sector **OPPORTUNITY:** It is an independent and regulated administrative authority that guarantees the interoperability of communication security, which would limit the emergence of multiple "private" V2G root CAs
4. Complexity of implementation and deployment	**STRENGTH:** Simple implementation due to the uniqueness of the solution and its management by a unique actor and decision-maker. At the technical level, this architecture is simple to deploy. **WEAKNESS:** It is a complex architecture because it does not necessarily depend on a unique actor and it involves a form of regulation that can take a long time to put in place. **Threat:** In the event of a forced replacement of the *V2G Root CA* - "Certification System Manager", the delays in setting up the call for tenders and in appropriating or modifying the IT system can lead to malfunctions and a decrease in the quality of the system.

5. Existence of barriers to entry to be *V2G Root CA*	**OPPORTUNITY:** Regulation favours a unique *V2G root CA* for governance, which severely limits the possibility for a new player to establish itself as *V2G root CA*. **OPPORTUNITY:** The operational management of certificate generation can be managed by a third-party IT actor through calls for tenders. **OPPORTUNITY:** The implementation of a *V2G Root CA* - "Auditor" allows to ensure a follow-up of the quality of service of the IT system manager.
6. Scalability of the system	**STRENGTH:** The private key allowing the certification of actors remains the property of the governance authority and is not dependent on an economic actor. **WEAKNESS:** Possibility of compromising the architecture if the private key is discovered by the certification system manager. **Threat:** The uniqueness of the V2G Root CA and the IT system hinders creativity and initiative in improving and securing implemented processes.
7. Economic and technical resilience of the *V2G Root CA*	**STRENGTH:** The potential separation of roles of the *V2G root CA*, and the non-economic nature of the governance authority, makes this architecture more resilient in the face of the disappearance of the certification operator or audit operator. **STRENGTH:** The potential separation of roles of the *V2G root CA*, and the non-economic nature of the governance authority, makes this architecture transparent to the certification operator's compromise and makes it easier for them to upgrade their security level or recover it after being compromised. **STRENGTH:** In order to ensure a cybersecurity of the system, cybersecurity criteria can be integrated into the specifications when issuing the call for tenders for the management of the IT certification system.

7.3. MF Architecture: A federation of cross certification

7.3.1. Description

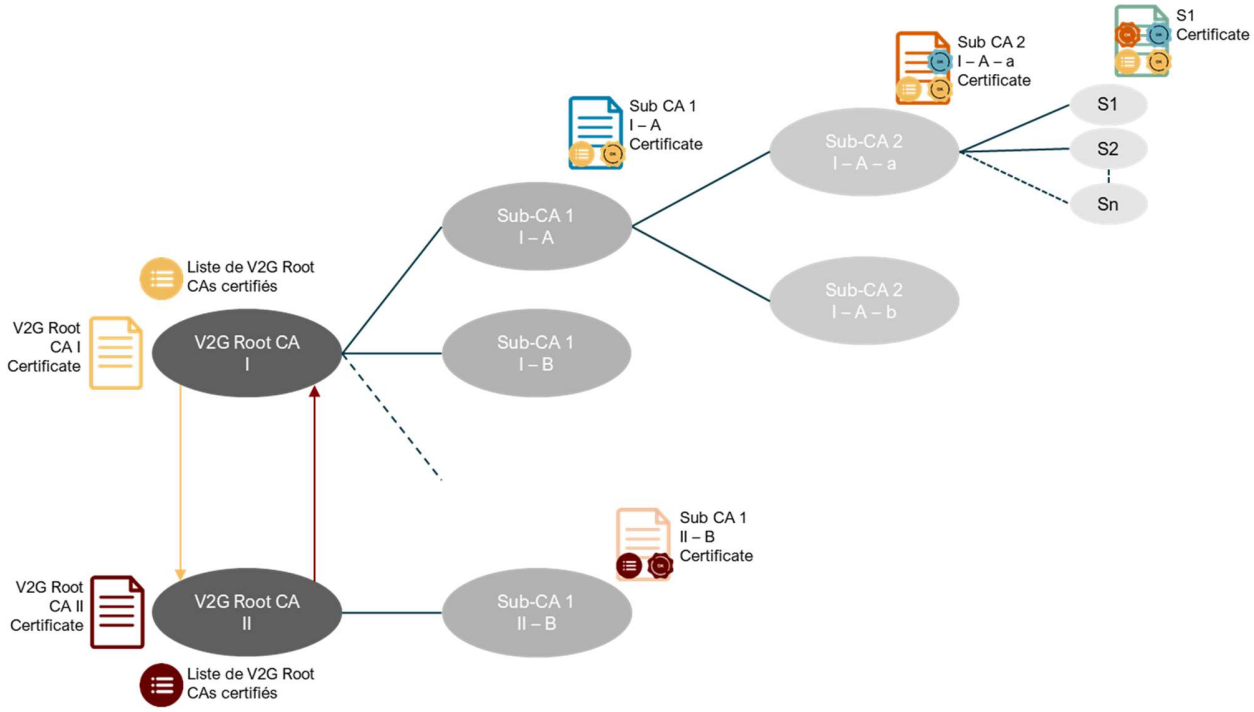

Figure 4 - Block diagram of the MF architecture " A federation of cross certifications".

In this architecture, there is not one but several *V2G Root CAs* that coexist and whose legal structure is not imposed. They can be, for example, regulated authorities, market companies, consortia and business groups or even private or public bodies. Each *V2G Root CA* manages its own certification chain in a way comparable to UF or UR architectures: each *V2G Root CA* defines its own governance rules and tariffs. However, a bilateral link between *V2G Root CAs* is required to ensure system interoperability. Each new entrant wishing to offer a V2G Root CA service must achieve cross certifications with all existing *V2G Root CAs* (or at least those managing the geographical area of interest).

Let us consider the example described in the introductory section with a *V2G Root CA* operating on the UF architecture principle (i.e. an economic, commercial and unregulated actor) and a second *V2G Root CA* operating on the UR architecture principle (i.e. a neutral, regulated and non-commercial actor whose IS is managed by an external and audited provider). When establishing the contractual link between the two *V2G Root CAs,* each *V2G Root CA* updates[14] its own unique list of trusted V2G Root CAs (*trust list*) and sends it to the actors under its authority. This list can be integrated into the *V2G Root CA* Certificate, or otherwise transmitted in parallel with it. The

[14] The mechanism for managing *trust lists* is not specified in ISO 15118. The process of transferring, securing, updating and decrypting *trust lists* remains to be defined for PnC.

listed *V2G Root CAs* are thus considered as sub-authorities and their certification is considered valid. The interoperability of the systems is ensured as explained in the following examples.

When the European *CSO* is certified by its *V2G Root CA*, then the French subsidiary is certified by its parent company and then the charging infrastructures by the subsidiary, the *trust lists* are integrated and shared in the certificates passing between the different levels. Thus, each charging infrastructure has at its disposal the signature of its "official" *V2G Root CA* as well as the *trust list* containing all the other accepted *V2G Root CAs.*

After connecting the electric vehicle to the charging infrastructure, the latter sends its *Contract Certificate*. The charging infrastructure checks that this contract is signed by the official *V2G Root CA* having signed its *leaf certificate* or, failing that, by a *V2G Root CA having* information on the *trust list at* its disposal. In the event of success, a bond of trust is therefore established between the two.

It should be noted that each *trust list* is unique and is associated with a unique *V2G Root CA* that signs it; there are therefore as many *trust lists* as there are *V2G Root CAs* and therefore as many possible combinations.

7.3.2. MF Architecture Evaluation Criteria

Criteria	Evaluation on both axes (internal and sector)
Number of *V2G Root CA*	N
Legal structure of the *V2G Root CA*	Several entities with different legal structures may coexist (neutral and regulated authority, commercial enterprise, association, public or private body)
1. Transparency of the *V2G Root CA*	**STRENGTH:** Governance rules are specific to each *V2G Root CA*. **STRENGTH:** Each *Sub-CA 1* has a large panel of *V2G Root CAs* to choose the governance rules and prices that suit it. **WEAKNESS:** Lack of transparency on the governance rules of *V2G Root CAs*. **WEAKNESS:** Lack of tariff transparency; each *V2G Root CA* sets its own tariffs and tariff rules. **OPPORTUNITY:** Competition between *V2G Root CAs* will allow a homogenization of governance rules, tariffs and tariff rules.
2. Distribution of the functions of the *V2G Root CA*	**STRENGTH:** Each *V2G Root CA* is free to choose its operating system. **WEAKNESS:** The audit of *V2G Root CAs* is not mandatory. **OPPORTUNITY:** Competition between *V2G Root CAs* will allow a homogenization of the audit rules of *V2G Root CAs* and *Sub-CA 1*.
3. System interoperability	**STRENGTH:** Within the same architecture, interoperability is total. The use of *trust lists* makes it possible to extend this interoperability to other actors but **WEAKNESS:** the multiplicity of *trust lists* can be a constraint to complete interoperability of the system. **WEAKNESS:** *The* size of the *trust lists* increases with the number of interoperable *V2G Root CAs.* Updating these *trust lists* can quickly become a limiting factor in the deployment of an interoperable system. **WEAKNESS:** The processes for interpreting trust lists are not defined in ISO 15118. Interoperability cannot work (at European and global level) without convergence of *trust list* reading algorithms (at European and global level respectively).

4. Complexity of implementation and deployment	**WEAKNESS:** The deployment of this architecture can be complicated and delayed by the consideration, formalization and development of protocols for creating, distributing, updating and interpreting *trust lists*. **WEAKNESS:** Maintaining the system in operational condition can be hampered by technical complexity due to the multiplicity of interoperability agreements.
5. Existence of barriers to entry to be *V2G Root CA*	**OPPORTUNITY:** Any new actor can declare himself *V2G Root CA*. **WEAKNESS:** For security reasons, *trust lists* must be updated at a defined frequency. The risk of security breaches increases with the frequency of updates. A waiting period should be considered for any new *V2G Root CA* wishing to join a *trust list*. **Threat:** This architecture will favour the *V2G Root CAs* capable of implementing a PKI architecture in a very short time and thus quickly capture as many *Sub-CAs as possible*.
6. Scalability of the system	**WEAKNESS:** System interoperability is achieved through bilateral agreements between *V2G Root CAs*. The frequency and disparity of *trust list updates* could introduce cybersecurity risks.
7. Economic and technical resilience of the *V2G Root CA*	**STRENGTH:** In the event of a *V2G Root CA* **crash**, the others continue to operate their system while remaining interoperable with each other. **STRENGTH:** In case of a *V2G Root CA* being compromised, it is removed from the *trust list of* all other *V2G Root CAs* with a bilateral agreement that continue to operate their system while remaining interoperable with each other. **Threat:** Since communication rules on security breaches are self-defined by each *V2G Root CA*, any breach of its IT systems is aggravated.

7.4. MR Architecture: A bridge administrative authority

7.4.1. Description

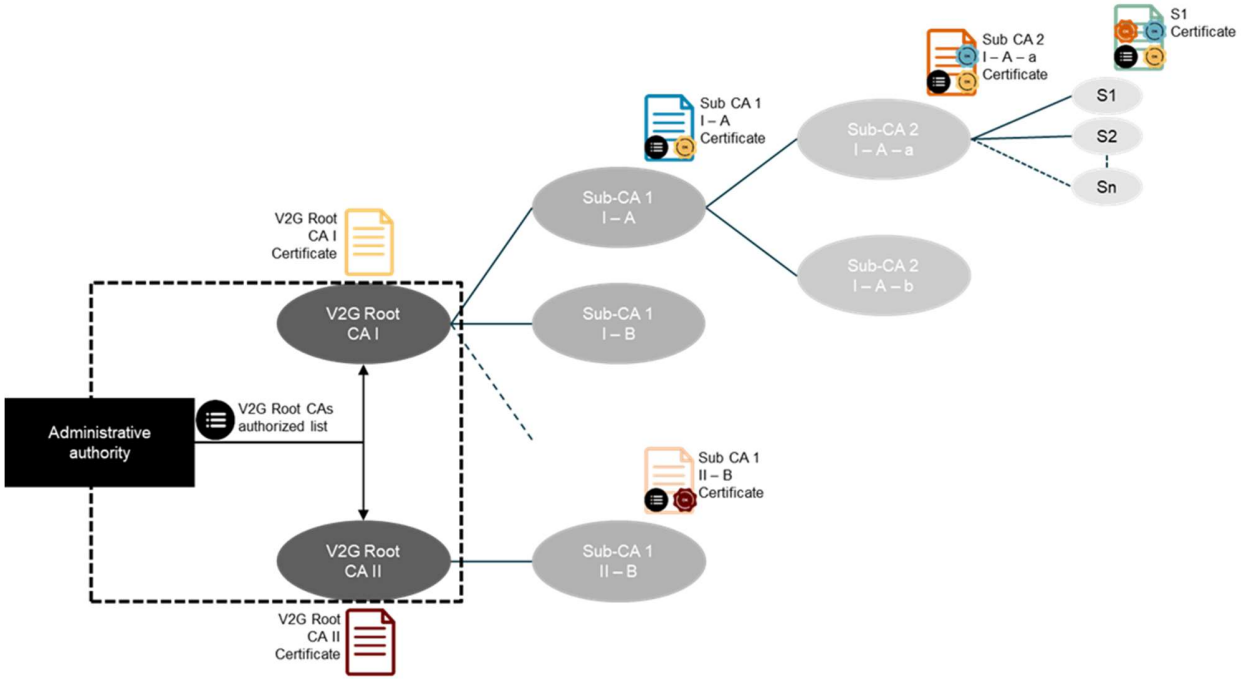

Figure 5 - Block diagram of the MR architecture "A bridge administrative authority".

This architecture is comparable to the MF architecture except that the list of *V2G Root CAs* certified (*trust list*) is managed and maintained[15] by an independent and neutral administrative authority without the technical skills required to manage the certification. In addition, this *trust list* is unique and common to all *V2G Root CAs* registered on it. In this architecture, the administrative authority sets minimum governance rules (RGM) applicable to any *V2G Root CA* wishing to join the *trust list* and therefore be interoperable with all *V2G Root CAs* already attached to the administrative authority. This authority also has the possibility to contract following a call for tenders with a specialized audit firm to certify and monitor the compliance of *V2G Root CAs* with RGMs. The audit of the remaining Sub-CA 1s by hand of each *V2G Root CAs*.

Each new entrant wishing to offer an interoperability service to its customers must approach the administrative authority which, after auditing and verifying compliance with the minimum governance rules, will update the *trust list* by adding this new entrant. This list will then be sent to all *V2G Root CAs* registered on it who are responsible for informing the actors depending on their architecture. This operation reduces the need for co-certification between *V2G Root CAs, which* simplifies the steps necessary to have a system that is both secure and interoperable.

[15] The mechanism for managing *trust lists* is not specified in ISO 15118. The process of transferring, securing, updating and decrypting *trust lists* remains to be defined for PnC.

As an example, let us consider the use case described in the introductory section with a European administrative authority. Let us consider here three *V2G Root CAs* of different legal structures that we will name *V2G Root CA 1*, *V2G Root CA 2* and *V2G Root CA 3*. In addition, let's assume that *V2G Root CA 3* is already registered on the *trust list*.

In order to make their systems interoperable on a large scale, the two *V2G Root CAs* (1 and 2) are approaching the administrative authority to apply for membership on the *trust list*. It starts an audit process to verify that its rules of governance (RGM) are respected by each *V2G Root CA*.

Three use cases are possible:

- The *V2G Root CA 1* does not comply with the minimum governance rules: it is not included in the list. This *V2G Root CA* will not be able to access the interoperability service via the administrative authority and is invited to renew its request after improving its governance rules,
- The *V2G Root CA 2* complies with the minimum rules of governance: it is included in the *trust list*, which is updated and transmitted to all stakeholders. This *V2G Root CA* will therefore be able to offer an interoperability service to its customers via the administrative authority,
- The *V2G Root CA 3*, already registered on *the trust list*, is compromised, goes bankrupt or no longer complies with the minimum governance rules imposed by the administrative authority: it is therefore removed from the *trust list*. This is updated and all "trusted actors" are informed. *V2G Root CA 3* will no longer be able to access the interoperability service via the administrative authority.

With the transmission of the *trust list* to the *V2G Root CAs* attached to the administrative authority, the listed *V2G Root CAs* are considered as sub-authorities and their certification is considered valid. This is how system interoperability will work.

When the European *CSO* is certified by its *V2G Root CA*, then the French subsidiary by its parent company and then the charging infrastructures by the subsidiary, the *trust lists* are integrated and shared in the certificates passing between the different levels. Thus, each charging infrastructure has at its disposal the signature of its "official" *V2G Root CA as* well as the *trust list* containing all the other accepted *V2G Root CAs.*

After connecting the electric vehicle to the charging infrastructure, the latter sends its *Contract Certificate*. The charging infrastructure checks that this contract is signed by the official V2G Root CA having signed its *leaf certificate* or, failing that, by a *V2G Root CA* having information on the trust list at its disposal. In the event of success, a bond of trust is therefore established between the two.

7.4.2. MR Architecture Evaluation Criteria

Criteria	Evaluation on both axes (internal and sector)
Number of *V2G Root CA*	N
Legal structure of the *V2G Root CA*	Several entities with different structures may coexist (neutral and regulated authority, merchant company, association, public or private body)
1. *Transparency of the V2G Root CA*	**STRENGTH:** Implementation by an administrative authority of minimum governance rules to be respected by all *V2G Root CAs* wishing to have an interoperable system via the *trust list* system. **STRENGTH:** Governance rules are specific to each *V2G Root CA*. **STRENGTH:** Each *Sub-CA 1* has a large panel of *V2G Root CAs* to choose the governance rules that suit it. **WEAKNESS:** Multiplication of governance complexities due to 2 governance bodies (administrative authority and *V2G Root CA*). **WEAKNESS:** Lack of transparency on the governance rules of *V2G Root CAs*. **WEAKNESS:** Lack of tariff transparency; each *V2G Root CA* sets its own tariffs and tariff rules **OPPORTUNITY:** Competition between *V2G Root CAs* will allow a homogenization of governance rules, tariffs and tariff rules.
2. Distribution of the functions of the *V2G Root CA*	**STRENGTH:** Each *V2G Root CA* operates its own system to generate *V2G Root CA Certificates* and establishes governance rules. **STRENGTH:** The administrative authority audits the *V2G Root CAs* and only includes in the *trust list* those that comply with minimum governance rules. **OPPORTUNITY:** Competition between *V2G Root CAs* will allow a homogenization of the audit rules of *V2G Root CAs* and *Sub-CA 1*.
3. System interoperability	**STRENGTH:** Interoperability is managed by a neutral authority, mutual co-certification between V2G Root CAs is no longer necessary for the roaming. **OPPORTUNITY:** Possibility to integrate new trusted *V2G Root CAs at* any time thanks to the neutrality of the administrative authority and the acceptance process.

	OPPORTUNITY: The *trust list* makes it possible to make pre-existing non-interoperable architectures interoperable without fundamentally changing their structure. All you have to do is update the *trust list*. **Threat:** Encourages the multiplication of *V2G Root CAs which* could generate complexities in roaming management.
4. Complexity of implementation and deployment	**WEAKNESS:** The deployment of this architecture can be complicated and delayed by the consideration, formalization and development of protocols for creating, distributing, updating and interpreting the *trust list*. **WEAKNESS:** Maintaining the system in operational condition can be hampered by technical complexity due to the multiplicity of requests for interoperability agreements. **Threat:** Encourages the multiplication of *V2G Root CAs* (different governance rules, different IT systems, a *trust list* that is increasingly difficult to maintain regularly).
5. Existence of barriers to entry to be *V2G Root CA*	**OPPORTUNITY:** Any new actor can declare himself *V2G Root CA*. **WEAKNESS:** For security reasons, the *trust list* must be updated at a defined frequency. The risk of security breaches increases with the frequency of updates. A waiting period should be considered for any new *V2G Root CA* wishing to join a *trust list*.
6. Scalability of the system	**WEAKNESS:** The interoperability of the systems requires an update of the *trust list* at the level of the IT systems of all the *V2G Root CAs*. The frequency and disparity of *trust list updates* could introduce cybersecurity risks.
7. Economic and technical resilience of the *V2G Root CA*	**STRENGTH:** In the event of a V2G Root **crashing**, the others continue to operate their system while remaining interoperable with each other but **WEAKNESS:** an update of the *trust list* is necessary. **STRENGTH:** In the event of a *V2G Root* being compromised, the others continue to operate their system while remaining interoperable with each other but **WEAKNESS:** an update of the *trust list* is necessary. **Threat:** Since the rules of communication on security breaches are self-defined by each *V2G Root CA*, it worsens any **compromising of** one or more IT systems

8. Appendix - Example of MR architecture implemented for the connected vehicle C-ITS

With the objective of gradually deploying vehicle communication interoperability (V2V), with the aim of starting an industrialisation phase before the end of 2020, the European Commission has set up itself as the governance authority for the C-ITS V2X solution. It is available to actors wishing to be part of the test and industrialization phase that will evolve towards the implementation of independent *Root CA* (RCA). The acceptability of the C-ITS V2X solution is already high and some car manufacturers such as Volkswagen are already deploying this solution in their models. It should be noted that this test phase is fully funded by the EC.

In order to provide a clear framework and governance for the deployment of the solution, a *Multi-Regulated* PKI architecture has been implemented by the EC. The EC is *C-ITS certificate policy authority*. It issues a *Certificate Policy*, as the *Certificate Policy Authority* (CPA), which defines the rules of governance and organization of certified entities. As such, it approves or rejects *Root CA*'s applications on the basis of audits. The *Root CA* can be private or public, without limitation of number, except for a problem of increasing the weight of the Trust List and therefore of processing time.

The Trust List is a static file that is frequently updated and regularly downloaded by all objects related to the PKI architecture. This unique list is available on the CPOC website

In this context, it issued a call for tenders for the implementation of a Trust List Manager (TLM) solution that complies with the technical and governance specifications drafted by ETSI. This solution is currently managed directly by the EC, which can revoke a *Root CA* from the *European Certificate Trust List.*

On the other hand, in the PKI architecture used by the EC, a C-ITS Point of Contact is used as a user interface allowing the various entities attached to the architecture to access the ECTL (European Certificate Trust List), more commonly known as the *Trust List* (TL). The latter being independent of the TLM). The TLM and C-ITS Point of Contact are under the control of the EC but it can be envisaged that they may be under the control of two separate entities.

The Root CA certifies two authorities:

- An Enlistment Authority (EA): issues the enrolment / car identification certificates. This certificate, which has a limited lifetime, is issued during the life of the vehicle and not at the factory. They allow you to sign messages sent by the vehicle in WIFI or 5G and received by neighbouring vehicles. In order to prevent the tracking of a vehicle's travel history, the pseudonym certificate used to sign the message changes regularly. Each vehicle has several pseudonymous certificates (about a hundred per week).
- An Authorization Authority (AA): issues authorization certificates, i.e. certificates detailing the specific messages for the use of the vehicle that can be sent ("I have priority" for ambulances / fire brigade / police vehicles...,"I turn right" for all vehicles, «I turn red" for traffic lights...).
- The EA and AA must be operated separately to avoid vehicle traceability.

The CPA (*Certificate Policy Authority*) is the authority responsible for implementing certificate management policies and PKI authorization management. This authority is composed of public and private actors.

Before being included in the TL, each *Root CAs* must carry out a declaration procedure at the CPA, this procedure takes place online and in physics between the representatives of each party (This procedure must be repeated for any certificate renewal):

- In order to validate the veracity of documents sent online, the eID (*Electronic Identification*) / eIDAS (Electronic Identification *Authentication and Trust Services)* ID system is used by C-ITS to sign documents before sending them.
- For the physics phase, a *Root CA Authorized Representative (RCA AR*) must physically go to the CPA to authenticate himself and present his file. The CPOC *Authorized Representative* checks whether the specifications specified in the file are really within the scope of the Root CA.
- An audit of the compliance of the CPS (*Certification Policy Statement*) with the CP (Certificate Policy) issued by the CPA is carried out by an accredited auditor chosen by the EC.
- Once validated by the CPA and the CPOC, the Root CA certificate is sent to the TLM and then added to the Trust List.

Contact Information

Gilles Bernard

gilles.bernard@afirev.fr

22 Avenue Jean AICARD, 75011 Paris, France