Recommandation sur la sécurité de la communication pour l'itinérance de la recharge des véhicules électriques

Architectures PKI liées à la norme de communication borne-véhicule ISO 15118

1er novembre 2019

Sommaire

Résumé

L'objectif poursuivi par l'AFIREV dans le cadre de cette note de positionnement sur la sécurité de communication de l'itinérance de la recharge des véhicules électriques est de construire un consensus français sur la mise en place d'une architecture PKI liée à la norme de communication borne-véhicule ISO 15118. L'AFIREV souhaite proposer une architecture cible du fonctionnement de l'infrastructure d'échanges de clefs publiques (PKI) permettant un marché ouvert dans la gestion de ces clefs tout en garantissant un haut niveau de sécurité, de fiabilité et une simplicité d'usage ainsi qu'une efficacité économique pour le client final. Dans le cadre de cette démarche l'AFIREV a aussi souhaité aborder l'organisation et la gestion des plateformes d'échanges de certificats de contrat de mobilité (*contract certificate pools*) ainsi que l'enjeu du chargement de ces certificats dans les véhicules. La finalité recherchée étant de lancer des travaux à l'échelle de l'Union Européenne pour préparer une interopérabilité maximale des fonctions proposée par l'ISO 15118.

L'AFIREV a mené une analyse des forces et faiblesses mais aussi des opportunités, (SWOT) des quatre architectures possibles pour l'organisation de la chaine de confiance permettant la certification (Root CA - Sub CAs – Certificate user) :

- une autorité de certification unique et marchande
- une autorité de certification unique régulée à l'échelle européenne ou internationale
- une fédération de certifications croisées entre autorités marchandes
- une autorité administrative pont autorisant plusieurs autorités de certification régulées

L'AFIREV a évalué ces architectures sur des critères de transparence, d'interopérabilité, de complexité ou de résilience.

En conclusion l'AFIREV préconise une architecture Multi-Régulée basée sur une autorité administrative pont autorisant plusieurs autorités de certification régulées. Il est à noter que c'est le choix de la Commission Européenne pour les communications véhicule à véhicule (C-ITS). Cette architecture est une cible à atteindre en se basant sur la situation actuelle de coexistence de plusieurs architectures Unique-Libre avec des autorités de certification marchandes et pas nécessairement interopérable. Pour assurer cette transition l'AFIREV a émis plusieurs recommandations pour initier des discussions à l'échelle européenne, principalement sur les règles de gouvernance de cette architecture cible incluant le sujet des plateformes mais aussi sur les exigences techniques associées. L'AFIREV a également étudié l'organisation pour le chargement des certificats de contrats dans les véhicules assurant l'équité des conditions pour les opérateurs de mobilité et les constructeurs automobile. Une recommandation est faite à cet effet concernant la structure des plateformes d'échanges de certificats, sa compatibilité avec l'architecture multi-régulée et la gestion de ces chargements (cf. chapitre 5). L'AFIREV souhaite maintenant recueillir les avis et les réflexions des parties intéressés. Par la suite l'AFIREV souhaite travailler au travers d'un projet collaboratif avec la filière électromobile européenne à la construction d'une position consensuelle détaillée sur la gouvernance de cette architecture PKI. Cette position sera proposée à la Direction Générale mobilité et transport de la Commission Européenne.

1. Introduction

L'Association Française pour l'Itinérance de la Recharge Électrique des Véhicules (AFIREV), a été créée à l'initiative du Ministre de l'Économie, de l'Industrie et du Numérique lors du Mondial de l'Automobile de Paris en octobre 2014 et officialisée en mars 2015 par 7 acteurs majeurs de la mobilité électrique : Bolloré BS, Bouygues Énergies Services, Engie Ineo, Gireve, Renault, Izivia (Groupe EDF), Vinci Energies. Se sont joints à eux à ce jour : la FNCCR, Freshmile, Easytrip, Chargemap, Spie, PSA, VEDECOM, Total EV charge, DKV France et IER ; ainsi que des tiers intéressés : école des Ponts Paristech, Solstyce, Schwartz & Co. Son objet est de fédérer les initiatives qui concourent au déploiement de l'interopérabilité des services de recharge et de mobilité électrique en France pour en créer et maintenir les éléments communs entre ses acteurs, en représenter les intérêts auprès des autorités réglementaires, assurer la compatibilité internationale des solutions, et défendre le point de vue français vis-à-vis des initiatives et instances européennes de même nature.

Cette note de positionnement expose les recommandations de l'AFIREV quant à la mise en place d'une organisation entre acteurs pour l'échange de clés et de certificats (architecture PKI) sécurisant la recharge de véhicules électriques utilisant la norme de communication ISO 15118. Ces recommandations concernent en premier lieu la France mais avec une vision d'intégration et d'interopérabilité en Union Européenne et sur le continent européen. Ce document s'intéresse à la fois à l'architecture de génération des certificats et clés de sécurité (chaîne *V2G Root CA*, *Sub-CA 1*, *Sub-CA 2*, Sn) et à la mise à disposition de ces éléments (gestion de *pools*). Il décrit les principales architectures possibles sur la base des documents de la norme et de l'état de l'art décrit par la filière électromobile :

- 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, Juillet 2019

Ce document analyse les forces et les faiblesses inhérentes à chaque architecture ainsi que les opportunités et les menaces qu'elles peuvent représenter pour la filière électromobile. Finalement ce document émet une recommandation de la filière française pour une architecture PKI et sur la feuille de route pour la déployer en Europe et propose une vision de structuration des pools complétant les architectures retenues.

[1] ElaadNL est un centre de recherche commun à plusieurs gestionnaires de réseaux néerlandais dans le domaine des infrastructures de recharge intelligente des véhicules électriques.
[2] La VDE est la « fédération allemande des industries de l'électrotechnique, de l'électronique et de l'ingénierie de l'information »

2. Définitions

Architecture PKI : Architecture de gestion de *Public Key Infrastructure* (PKI), c'est une architecture de gestion d'une infrastructure à clés publiques (ICP). C'est l'architecture (organisation, gouvernance, procédures) permettant de gérer un ensemble de composants physiques (ordinateurs, serveurs) et de logiciels destinés à gérer les clés publiques des utilisateurs d'un système, ici le système de recharge de véhicules électriques en itinérance basé sur la norme ISO 15118. *Source Wikipédia*[3]

Certificat : Document électronique qui utilise une signature numérique pour lier une clé publique à une identité. Source *ISO 15118*

Clé publique/ privée : Les clés publique et privée sont utilisées en cryptographie asymétrique, il y a deux clefs de chiffrement, telles que si l'utilisateur utilise une première clef dans un algorithme dit « de chiffrement », la donnée devient inintelligible à tous ceux qui ne possèdent pas la deuxième clef. On peut retrouver le message initial lorsque cette deuxième clef est donnée en entrée d'un algorithme dit « de déchiffrement ». Par convention, on appelle la clef de déchiffrement la clef privée et la clef de chiffrement la clef publique. La clef qui est choisie privée n'est jamais transmise à personne alors que la clef qui est choisie publique est transmissible sans restriction. *Source Wikipédia*[4]

Itinérance de la recharge : Faculté pour l'utilisateur, titulaire ou non d'un contrat ou d'un abonnement avec un opérateur de mobilité, d'utiliser les réseaux de recharge de différents opérateurs d'infrastructure de recharge sans inscription préalable auprès de l'opérateur exploitant le réseau dont il utilise ponctuellement le service de recharge, soit en ayant accès à la recharge et au paiement du service par l'intermédiaire d'un opérateur de mobilité avec lequel il a un contrat ou un abonnement, soit en ayant accès à la recharge et au paiement du service directement auprès de l'opérateur de l'infrastructure à laquelle il recharge son véhicule. Source *Décret n° 2017-26 du 12 janvier 2017*

***Leaf certificate* :** Tout certificat ne pouvant être utilisé pour signer d'autres certificats. Par exemple : Certificats client et serveur TLS / SSL, certificats de courrier électronique et tout certificat d'entité finale. *Source Wikipédia*[5] C'est donc le dernier niveau de certificat délivré sur la chaîne des PKIs. Dans le cas traité ici, un certificat de contrat de services de mobilité et un certificat de point de recharge sont des *leaf certificates*.

***Opérateur de mobilité* (*eMSP)* :** *electro-Mobility Service Provider* –

- Entité avec laquelle un utilisateur contractualise afin d'avoir tous les services liés aux VE. *Source ISO 15118*
- Prestataire de services de mobilité pour les utilisateurs de véhicules électriques incluant des services d'accès à la recharge. *Source Décret n° 2017-26 du 12 janvier 2017*

[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

Opérateur d'infrastructure de recharge (CSO) : *Charging Service Operator –*

- Opérateur d'infrastructure de recharge – Acteur responsable de l'installation, de l'O&M des infrastructures de recharge (incluant les places de stationnement associée) et de la gestion de l'achat d'électricité permettant de répondre à la demande en énergie aux bornes. *Source ISO 15118.* En réalité, dans l'organisation traitée ici, le CSO est l'acteur qui exploite l'infrastructure de recharge pour autoriser l'accès des utilisateurs et assurer la recharge définie dans son service.
- *Personne qui exploite une infrastructure de recharge pour le compte d'un aménageur ou pour son propre compte. Source Décret n° 2017-26 du 12 janvier 2017*

Opérateur d'itinérance (Plate-forme d'interopérabilité) : opérateur qui concourt au déploiement de l'itinérance de la recharge en facilitant, sécurisant et optimisant les échanges de données entre les opérateurs d'infrastructure de recharge et les opérateurs de mobilité. *Source Décret n° 2017-26 du 12 janvier 2017*

Pool : Entité où les acteurs vont déposer leurs informations numériques publiques afin de pouvoir associer les informations rapidement et simplement.

Root certificate : certificat racine – certificat de clé publique qui identifie une autorité de certification racine – *Source Wikipédia*[6]

Sn **:** Elément physique placé en fin de la chaîne PKI et disposant du leaf certificate. Dans le cas traité ici, il s'agit d'un véhicule, d'un point de recharge ou d'un contrat de services de mobilité.

Sub CA **:** *Subaltern Certificate Authority,* autorité délivrant un certificat de sécurité basé sur un certificat racine d'une architecture PKI pour le service de recharge entre véhicule électrique et borne de recharge. La norme ISO 15118 prévoit que 2 niveaux de *Sub-CA* sont possibles derrière un *V2G Root CA* : le *V2G Root CA* certifie le *Sub-CA 1* qui lui-même certifie le *Sub-CA 2*. L'attribution de rôles de Sub CA est proposée dans ce document.

Trust List **:** La trust list liée à un certificat est une liste prédéfinie d'éléments signée par l'entité émettrice du certificat. Cela peut être une liste de noms ou de fichiers, tous les éléments qu'elle contient sont authentifiés et considérés de confiance par l'entité émettrice.

V2G root CA : *Vehicle-to-grid root Certificate Authority,* délivrant le certificat de sécurité racine d'une architecture de PKI pour le service de recharge entre véhicule électrique et borne de recharge. Le V2G root CA et tous les acteurs qui reçoivent de lui des certificats et les utilisent doivent s'inscrire dans une même gouvernance avec ses règles.

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

3. Liminaire

3.1. Cette note répond à une problématique exposée par la filière

La mise en place et la gestion d'architectures PKI ISO 15118 permettant une sécurisation des échanges et authentification automatique entre véhicule, contrat de mobilité et infrastructures de charge présente aux yeux de la filière plusieurs problématiques auxquelles ce document ambitionne de répondre. Ces problématiques ont été identifiées par les membres de la filière représentés au sein d'AFIREV et part l'étude de l'état de l'art présenté en introduction.

Les problématiques de marché

De nombreux acteurs de la filière électromobilité sont convaincus que son essor est dépendant

- du niveau d'ouverture des réseaux d'infrastructure de recharge,
- de la mise en place de conditions d'accès au marché transparentes et équitables pour les opérateurs de service comme d'infrastructure,
- de la capacité de la filière à échanger de l'information temps réelle sur l'utilisation de l'infrastructure de recharge et les services,
- de l'alignement sur des normes et de protocoles de communication communs et interopérables.

La cyber sécurité de la communication autour de la recharge des véhicules électriques est un sujet transverse à ces dépendances. Le niveau de contribution des acteurs publique et des régulateurs sur cet axe de travail cyber sécurité, notamment pour lever certaines barrières, est un sujet discuté au sein de la filière et c'est un des éléments abordés dans cette note.

Les barrières à l'entrée que pourrait poser des mécanismes d'authentification reposant sur une PKI, comme celui de la norme ISO 15118 discuté dans ce document, sont des sources d'inquiétude pour certains acteurs. L'AFIREV souhaite au travers de ce document proposer des solutions d'architecture et de gouvernance levant ces inquiétudes.

Le travail réalisé par l'AFIREV vise, entre-autre, à initier des discussions sur des architectures PKI qui répondent aux attentes des acteurs de la filière en permettant de limiter les positions monopolistique et oligopolistique. Les travaux de l'AFIREV s'inscrivent dans un fonctionnement de l'itinérance de la recharge reposant principalement sur des plateformes d'interopérabilité.

L'AFIREV est convaincue que les travaux d'élaboration de l'architecture PKI complétant la norme ISO 15118 sont nécessaire car inexistant et doivent reposer sur un travail collectif de la filière portée à une échelle européenne et non le travail d'un petit nombre d'acteurs intéressés et à une échelle nationale risquant une complexification mortelle pour l'ISO 15118.

Il n'y a pas encore de consensus au sein de la filière sur l'entité ou les entités en charge de la gouvernance, la mise en place et la gestion de l'architecture PKI. A contrario de nombreux acteurs semblent convaincus qu'une implication des régulateurs aiderait à structurer l'écosystème. La

profondeur de cette implication restant à définir : gouvernance, définition de l'architecture, gestion de l'architecture, etc.

La gestion d'une architecture PKI à plusieurs *root* ou d'une architecture à *root* unique est aussi un sujet à débat que souhaite éclairer l'AFIREV au travers de ce document.

Les problématiques techniques : IT et cyber sécurité

C'est une évidence pour la filière que l'avenir des IRVE est d'être connectées et d'offrir de multiples services digitaux. Un système robuste (avec attestation des identités, confidentialité et assurance d'intégrité des message) de gestion de l'authentification pouvant accompagner l'essor de la mobilité électrique semble donc indispensable à de nombreux acteurs de l'écosystème. La sécurité et la confiance des communications borne – véhicule étant un pilier des services de recharge car intimement liés aux mécanismes de paiement. Au-delà de l'interopérabilité côté utilisateur, véhicules, EMSP, …, ce système de gestion de l'authentification doit aussi être transparent vis-à-vis du parc d'IRVE d'un CPO et donc s'interopérer avec plusieurs constructeurs de bornes.

La solution technique *Autocharge* est évoquée comme alternative à l'utilisation de l'ISO 15118 avec des PKI pour réaliser la fonction de *Plug and Charge.* Cette solution repose sur l'identification du véhicule par la borne de recharge au travers de l'adresse MAC (unique) du dispositif de communication de ce véhicule. Comme le *Plug and Charge* ISO 15118, l'*Autocharge* permet une meilleure expérience utilisateur de la recharge et une meilleure cybersécurité en supprimant le badges RFID (aisément falsifiable).

L'*Autocharge* permet un meilleur niveau de sécurité car il est plus difficile de répliquer une adresse MAC qu'un badge RFID mais ce n'est pas une méthode d'identification sécurisée qui protègerait de l'interception de l'identifiant utilisateur. De même l'*Autocharge* ne permet pas de gérer les identifiants compromis ni ne permet l'encryptions de l'identifiant. Bien que l'*Autocharge* soit une solution plus simple à implémenter, la protection contre la fraude offerte par cette solution technique est jugée comme insuffisante en comparaison avec un protocole de communication comme l'ISO 15118

La filière semble convaincue que l'utilisation de la norme de communication borne-véhicule ISO 15118 garantit un niveau de sécurité élevé à condition de pouvoir y assortir une architecture PKI robuste. La filière est aussi convaincue que la solution « PKI » est la meilleure.[7]

Des craintes subsistent sur certains aspects techniques de la gestion des certificats d'authentification des contrats de mobilité que certains acteurs de la filière considèrent comme trop dépendante des constructeurs automobiles avec un risque de rendre les clients de ces constructeurs trop captifs.

Il a semblé aussi important pour l'AFIREV de souligner que les CPO n'ont pas encore été répertoriés comme « opérateur de services essentiels »[8] au sein de l'UE mais que cette possibilité

[7] 89% de réponse positive au questionnaire STF (voir chapitre 1. Introduction)
[8] Directive européenne (UE) 2016/1148

future doit être envisagée dans la réflexion sur les architectures en construction en lien avec la cyber sécurité.

Points d'amélioration préalablement identifiés par la filière

Plusieurs acteurs de l'écosystème de la recharge pointent des insuffisances de la norme ISO 15118 (principalement de sa partie 2) sur sa capacité à définir une architecture PKI apportant une sécurité des communications de la recharge renforcée, fonctionnelle et que l'on puisse passer à l'échelle.

L'AFIREV souligne que certains de ces aspects ne peuvent être totalement ou en partie couvert par une norme ISO mais relève de règles d'organisation à traiter par le marché et/ou par la réglementation. Ces éléments sont bien manquants et rendent difficile le déploiement d'une sécurité de communication de l'itinérance de la recharge suffisante et facilement capable de passer à l'échelle mais ils doivent être définis par la filière en complément des normes ISO. L'objet de ce document étant d'initier une partie de ces réflexions.

En termes de gouvernance, le manque d'exigences définies pour établir la chaîne de confiance, dans ou en dehors de l'ISO 15118, ainsi que de descriptions des processus de certification mais aussi de révocation de certification affaiblissent les mécanismes de sécurité et complexifie la mise en place des mécanismes d'authentification automatique.

Les incertitudes techniques comme la gestion de 2 ou 3 niveaux de certification au choix sont aussi des sources d'affaiblissement et de complexité.

Les complexités restantes, car non intégralement adressées, dans la gestion des cycles de vie des certificats et dans l'interaction de l'utilisateur finale avec ces certificats sont aussi des freins à lever pour proposer une architecture permettant une communication borne-véhicule sécurisée.

Ce document de recommandation traite uniquement de la chaîne de certifications et de signature garantissant la confiance et la sécurité des échanges entre acteurs ainsi que de la circulation de ces certificats[9] pour vérification sur des plateformes (*pools*). Cependant, il ne traite pas de l'architecture informatique et de télécommunication pour la distribution, la mise à jour et la révocation des certificats, dans les véhicules, les bornes et les systèmes d'informations des différentes parties prenantes de la recharge itinérante de véhicules électriques. Il vise à proposer des recommandations pour rassembler les acteurs de la filière autour d'une position commune sur la meilleure solution de gestion des PKI de l'écosystème de recharge en termes de gouvernance, de complexité, de coûts d'intégration, de cybersécurité, de passage à l'échelle et d'interopérabilité.

3.2. Architectures PKI étudiées

Dans cette note, quatre architectures PKI envisageables ont été analysées en se basant notamment sur le document Elaad[10], nous avons défini la nomenclature suivante

[9] Les périodes de validités des certificats ne seront pas abordées dans ce document
[10] *"Exploring the Public Key Infrastructure for ISO 15118 in the EV charging ecosystem" – eLAAD*

Unique indique une architecture basée sur un unique V2G Root CA

Multi indique une architecture basée plusieurs V2G Root CA

Régulée indique une architecture disposant d'une autorité régulatrice

Libre indique une architecture sans autorité régulatrice

Les architectures étudiées sont une combinaison de ces critères :

- **Architecture *Unique-Libre* (UL) : Une autorité unique et marchande**

  Dans cette architecture, le *V2G Root CA* est un acteur commercial qui est l'unique gestionnaire du système de certification (dans sa gouvernance et dans sa mise en œuvre IT) et qui est garant de son fonctionnement et de son interopérabilité. Il en édicte donc les règles de fonctionnement.

- **Architecture *Unique-Régulée* (UR) : Une autorité unique régulée à l'échelle européenne ou internationale**

  Dans cette architecture, le *V2G Root CA* est un acteur non commercial et régulé par une autorité publique (soit une autorité régulatrice européenne ou un consortium d'acteurs privés régulé par une instance européenne). Ce *V2G Root CA* peut répartir ses fonctions en trois parties :

  - Gouvernance (nous l'appellerons *V2G Root CA* – « Autorité régulatrice ») : fixe les règles de gouvernance et les applique de manière équivoque. Il est le propriétaire de la clé privée du *V2G Root CA* et est garant du bon fonctionnement du système de certification.
  - Opération de la certification (nous l'appellerons *V2G Root CA* – « Gestionnaire du système de certification ») : sélectionné suite à un appel d'offre émis par le *V2G Root CA* – « Autorité régulatrice », il gère le système IT. Il utilise la clé privée lors de la certification mais n'en a pas nécessairement connaissance. En se conformant aux normes en vigueur (ISO 27001, etc.) et aux exigences complémentaires de l'autorité de régulation.
  - Audit (nous l'appellerons *V2G Root CA* – « Auditeur ») : sélectionné suite à un appel d'offre émis par le *V2G Root CA* – « Autorité régulatrice », il audite le *V2G Root CA* – « Gestionnaire du système de certification » (audit à rendre public).

- **Architecture *Multi-Libre* (ML) : Une fédération de certifications croisées**

  Dans cette architecture, il n'existe pas un mais plusieurs *V2G Root CAs* qui coexistent et dont la structure juridique n'est pas imposée. Chaque *V2G Root CA* gère sa propre chaîne de certification de manière comparable aux architectures UL ou UR. Afin d'assurer l'interopérabilité des systèmes, un lien bilatéral entre *V2G Root CAs* est nécessaire. Chaque *V2G Root CA* crée et tient à jour sa propre *trust list*[11] intégrant tous les liens de confiance établis. Les *trusts lists* sont ainsi uniques par *V2G Root CA* et indépendantes les unes des autres.

[11] Le mécanisme de gestion des *trust lists* n'est pas spécifié dans l'ISO 15118. Le processus de transfert, de sécurisation, de mise à jour et de déchiffrage des *trust lists* reste à définir pour le PnC si les architectures C et/ou D sont retenues.

- **Architecture *Multi-Régulée* (MR) : Une autorité administrative pont**

  De même que dans l'architecture ML, il n'existe pas un mais plusieurs *V2G Root CAs* qui coexistent et dont la structure juridique n'est pas imposée. Chaque *V2G Root CA* gère sa propre chaîne de certification de manière comparable aux architectures UL ou UR. Cependant, contrairement à l'architecture *Multi-Libre*, l'interopérabilité des systèmes est gérée par une autorité administrative qui a pour mission de créer une *trust list* unique, de la tenir à jour et de la transmettre à tous les *V2G Root CAs* inscrits sur cette liste. Cette autorité fixe des règles de gouvernance minimales devant être respectées par tout nouveau *V2G Root CA* désirant intégrer la *trust list* pour être interopérable. Afin de vérifier le respect de ces règles de gouvernance minimales, l'autorité administrative publie un cahier des charges et fait appel à un cabinet d'audit spécialisé pour auditer les nouveaux prétendants et faire un suivi des membres listés.

Il est important de rappeler qu'il reste possible pour tout acteur de mettre en place une architecture PKI indépendante pour gérer la sécurité des échanges dans un service de recharge de véhicules électriques, et donc tout acteur économique reste libre de se constituer *V2G root CA*. En revanche la coexistence de multiples architectures de gestion PKI est un frein majeur à l'interopérabilité des services de recharge et donc à l'itinérance de la recharge. Une infrastructure de recharge publique qui serait rattachée à une telle architecture PKI indépendante ne respecterait donc pas l'article 12 du décret n° 2017-26 du 12 janvier 2017.

Un enjeu supplémentaire de cybersécurité est à considérer. Par définition la mise en place d'une architecture PKI permet de sécuriser les échanges de certificats. Toute cyberattaque sur le système entraînera nécessairement des défauts de fonctionnement graves pouvant mener à la suspension de la fonctionnalité Plug'n'Charge pendant une durée indéterminée. L'objectif de ce document n'est pas de donner des préconisations techniques sur la cybersécurisation du système IT mais il paraît judicieux d'estimer l'impact d'une compromission du système sur les architectures PKI considérées afin de soulever quelques points d'attention.

A titre d'exemple et pour illustrer chacune des architectures du document nous allons considérer l'exemple suivant :

- ***V2G Root CA* :** Une ou plusieurs autorité(s) de certification de certificat racine selon l'architecture, le nombre sera précisé dans la description de chaque architecture,
- ***Sub-CA 1* :** Un opérateur d'infrastructure de recharge (*CSO*) établi à l'échelle européenne,
- ***Sub-CA 2* :** Une filiale française de ce *CSO* opérant exclusivement des bornes sur voies rapides et autoroutes
- **S1 à Sn :** Un parc de n bornes sur voies rapides et autoroutes en France géré par ce *CSO*,
- **Un véhicule électrique** possédant un contrat de mobilité signé par le ou un des *V2G Root CAs.*

3.3. Méthode utilisée pour l'évaluation des architectures PKI

Les architectures seront évaluées sur 2 axes[12] :

- Avantages et inconvénients de cette architecture pour la filière de la recharge en itinérance de véhicules électriques : **OPPORTUNITE** ou **MENACE**
- Avantages et inconvénients intrinsèque de cette architecture pour l'acteur ou les acteurs opérant et gouvernant le V2G root CA : **FORCE** ou **FAIBLESSE**

et sur 10 critères :

Critère 1. Transparence du *V2G Root CA* :

Ce critère permet d'évaluer l'accessibilité des acteurs dépendant du *V2G Root CA* aux informations relatives à la gouvernance, aux grilles tarifaires, aux modalités contractuelles et aux règles de gestion des services du *V2G Root CA* (SLA, support, etc.). Il tient aussi compte de l'implication de ces acteurs par le *V2G Root CA* dans la définition et la rédaction des règles de gouvernances et des autres critères les impactant.

Critère 2. Répartition des fonctions du *V2G Root CA* :

Dans le fonctionnement de l'architecture PKI, le *V2G Root CA* tient un rôle central et assure trois fonctions principales qui peuvent être réparties entre plusieurs acteurs :

- Fonction « Gouvernance » : Le *V2G Root CA* – « Autorité de gouvernance » est chargé de définir le cahier des charges à respecter pour tout nouveau Sub-CA 1 désirant être certifié, détient la clé privée du *V2G Root CA* et se porte garant du bon fonctionnement de l'architecture PKI. L'acteur en charge de la gouvernance peut émettre des appels d'offres et sous-traiter les deux fonctions suivantes.
- Fonction « Opération de la certification » : Le *V2G Root CA* – « Gestionnaire du système de certification » est chargé d'opérer le

[12] Méthodologie SWOT

système IT permettant de certifier les acteurs. Il peut utiliser la clé privée pour la certification mais sans nécessairement en avoir connaissance.

- Fonction « Audit » : Le *V2G Root CA* – « Auditeur » est chargé d'auditer au niveau technique, politique et financier l'acteur réalisant la fonction « opération de la certification » et tout acteur désirant être certifié selon un cahier des charges définit par l'entité de gouvernance.

Critère 3. Interopérabilité du système :

L'interopérabilité repose sur la capacité des systèmes à échanger des informations et à fonctionner ensemble et sans couture. Ce critère permet d'analyser l'impact de la mise en place de l'architecture PKI considérée sur le fonctionnement de l'interopérabilité du système d'itinérance de la recharge. Il tient aussi compte de l'ouverture de l'architecture[13] à d'autres marchés, non européen par exemple.

Critère 4. Complexité d'implémentation et de déploiement :

Le déploiement des architectures ne se valent pas tant sur le plan technique (développements informatiques, complexité des processus, définition de nouvelles méthodes), sur le plan politique (acceptabilité par les parties prenantes, nécessité de réguler) ou encore sur le plan temporel (temps nécessaire à l'implémentation, temps nécessaire à la mise en place de l'architecture, temps nécessaire à la prise de décision). Ce critère permettra de jauger le reste à faire pour chaque architecture PKI considérée.

Critère 5. Existence de barrières à l'entrée pour être *V2G Root CA* :

Conformément aux règles de concurrence et aux règles anti-trust, tout nouvel acteur est en capacité de se déclarer V2G Root CA. Via ce critère nous analyserons les freins introduits par chaque architecture pour la création de nouveaux *V2G Root CAs*.

Critère 6. Évolutivité du système :

Chaque certificat a un cycle de vie qui lui est propre et qui peut différer selon l'architecture PKI retenue. Il est donc nécessaire d'évaluer la capacité du système à évoluer de manière sécurisée, c'est-à-dire accepter les remplacements ou mise à jour des certificats tout en assurant une sécurisation (physique et cyber) des processus.

[13] La norme ISO 15118 préconise la mise en place de 5 *V2G Root CAs* dans le monde (soit 1 par continent) et l'installation des 5 *V2G Root CA Certificates* dans chaque véhicule électrique

Critère 7. Résilience économique et technique du *V2G Root CA* :

La résilience d'un système correspond à sa capacité à surmonter des événements rares et perturbateurs sans impacter son niveau de fonctionnement. Pour chaque architecture PKI, nous évaluerons la résilience du *V2G Root CA* face à :

- Un événement perturbateur d'ordre économique : faillite du V2G Root CA, rachat du V2G Root CA par une autre société,
- Un événement perturbateur d'ordre technique : défaut du système de certification, compromission du V2G Root CA, cyberattaque.

Conformément à la norme ISO 15118, un *V2G Root CA* ne peut générer un *Leaf Certificate*, il est donc nécessaire d'avoir une architecture PKI avec à minima 3 niveaux de profondeurs (Root CA, Sub CA, Sn). Cette profondeur est aussi limitée à 4 par l'ISO 15118. Toutes les architectures considérées permettent d'avoir une structure maximale en termes de niveau de profondeur. Ce critère ne sera donc pas discriminant, il est donc volontairement mis à l'écart dans l'évaluation des architectures.

4. Synthèse de l'analyse et choix de l'architecture PKI

4.1. Quatre critères de sélection priorisés

L'analyse des 4 architectures réalisée selon les sept critères prédéfinis a permis de tirer des conclusions sur un choix d'architecture PKI cible en fonction de la priorisation de certains critères. L'AFIREV a priorisé les quatre critères les plus discriminants, les trois autres critères permettent une meilleure compréhension des enjeux de chaque architecture et ont été pris en compte lors de l'établissement des conclusions.

Les critères de sélection priorisés sont listés ci-dessous :

- **Critère 1. Transparence du *V2G Root CA* :**

  L'architecture PKI à mettre en place doit inciter à une transparence du ou des *V2G Root CAs* tant dans l'établissement des règles de gouvernances que dans le choix des tarifs et des règles tarifaires. La transparence du ou des *V2G Root CAs* permettrait d'assurer un système de certification stable et non discriminatoire.

- **Critère 3. Interopérabilité du système :**

  L'interopérabilité du système repose sur une coopération technique des systèmes IT et est notamment une base pour offrir aux clients une expérience sans couture de la fonction de recharge en PnC. L'architecture PKI retenue devra permettre d'assurer un service d'itinérance fiable, simple et sécurisé sur la zone géographique la plus large possible.

- **Critère 4. Complexité d'implémentation et de déploiement :**

  L'architecture retenue devra permettre un bon compromis entre :

  - une facilité de mise en place de la solution technique permettant un fonctionnement simple de l'architecture et du système de certification,
  - une prise de décision efficace avec la définition de règles de gouvernance convenant aux parties prenantes,
  - une rapidité de mise en place et de déploiement, avec des développements techniques et des prises de décisions réalisables dans un temps raisonnable.

- **Critère 7. Résilience économique et technique du *V2G Root CA* :**

  L'architecture retenue doit être résiliente sur le plan économique et le plan technique afin de permettre une pérennisation de l'architecture et la sécurisation des échanges de certificats. Le choix de l'AFIREV sera aussi motivé par une capacité intrinsèque de l'architecture à encourager une innovation permanente des processus mis en place ainsi qu'à assurer une supervision continue de l'existant.

4.2. Choix de l'architecture

L'étude AFIREV privilégie ainsi l'architecture MR reposant sur une autorité administrative pont autorisant plusieurs autorités de certification régulées.

Une architecture *Régulée* peut être vue comme une architecture fédératrice. La délégation de la gouvernance à une entité publique ou à un consortium privé mais régulé a pour avantage une transparence totale des règles de gouvernance et des tarifs, un système interopérable, résilient et avec une implémentation simple. En effet, la mise en concurrence des *V2G Root CAs* – « Gestionnaire du système de certification » via des appels d'offres permettra d'encourager l'innovation tout en réduisant les tarifs de certification. Les incitations à l'innovation seront d'autant plus grandes que les délais entre chaque appel d'offres seront courts. De plus, ce système de séparation des fonctions du *V2G Root CA* permet d'avoir une architecture résiliente tant sur le plan économique (le *V2G Root CA* – « Autorité de gouvernance » a une probabilité de faillite très faible ; le *V2G Root CA* – « Gestionnaire du système de certification » et le *V2G Root CA* – « Auditeur » peuvent être remplacés à tout moment) que sur le plan technique via la définition d'un cahier des charges précis lors de l'appel d'offres et le suivi de son respect dans le temps par toutes les parties prenantes.

Cependant, l'installation d'une autorité de régulation européenne risque d'être longue. Les temps nécessaires aux prises de décisions peuvent être assez longs du fait que plusieurs acteurs devront s'accorder. Ceci pourrait entacher la simplicité de fonctionnement de ce système. De plus, combinés à des raisons de sécurisation et de stabilité du système, les délais entre appels d'offrent risquent d'être élevés ce qui mènerait probablement à des systèmes IT de plus en plus décorrélés du marché. A ces freins s'ajoute le risque de conflit d'intérêt : en cas de gouvernance par un consortium privé régulé, un acteur du consortium peut-il gérer le système de certification ?

L'architecture *Multi-Régulée* incite à la coexistence de plusieurs *V2G Root CAs* et donc à avoir un système plus concurrentiel. De ce fait, cette architecture PKI encourage davantage les gestionnaires des systèmes de certification à innover et proposer des systèmes de plus en plus sécurisés tout en réduisant leurs tarifs. L'autorité administrative serait quant à elle garante d'une transparence minimale de tout *V2G Root CA* désirant être interopérable. En respectant des règles de gouvernances minimales (RGM), tous les *V2G Root CAs* inscrits sur l'unique *trust list* s'engagent à assurer un service d'itinérance viable. Quant aux temps de décisions, ceux-ci sont réduits du fait d'une gestion autonome de chaque architecture par son *V2G Root CA*. D'autre part, l'existence d'une autorité administrative en charge de la gestion de la *trust list*, et donc de l'interopérabilité, permet d'avoir un système résilient (économiquement et techniquement), non discriminatoire et ouvert à tout nouvel entrant dès que celui-ci respecte les RGMs.

Bien que l'architecture MR puisse paraître comme la solution de référence pour le déploiement d'une architecture PKI, celle-ci fait encore face à une complexité technique de taille : la gestion de la *trust list*. La technologie de *trust list* est communément utilisée dans des systèmes IT pouvant échanger des informations sans coupure et sans limite de taille de fichier, comme par exemple C-ITS (Chapitre 8). Cette technologie n'est cependant pas définie dans la norme ISO 15118. Or, dans cette architecture, l'itinérance dépend expressément de la gestion de cette *trust list*. Un enjeu majeur est donc la définition d'un cahier des charges commun à toute la filière pour

l'implémentation de mécanismes de mise en place d'une trust list, des processus de sécurisation de la liste, des protocoles de transfert et de mise à jour de cette liste ainsi que d'algorithmes sécurisés de décryptage. La mise en place d'une architecture type MR est donc contrainte par des temps de décision, de développements techniques et d'intégration potentiellement longs. Une analyse plus fine des solutions techniques envisageable pour une *trust list* ou en remplacement d'une *trust list* ainsi que des délais de rédaction d'un cahier des charges applicable à toute la filière et de la mise en place du mécanisme de gestion des *trust lists* est à mener.

La gestion des *trust list* dans l'architecture MR introduit une barrière technique à l'entrée pour des bornes ou véhicules conçus pour des marchés fonctionnant avec des *V2G root CAs* sans *trust list* (architecture UL ou UR). En effet il est nécessaire que bornes et véhicules soient en mesure de manipuler cette *trust list* (codage, décodage, interprétation, mise à jour, révocation…), une mise à jour logicielle sera donc nécessaire en plus de la mise à jour des certificats pour les utiliser sur une plaque européenne disposant d'une architecture PKI de type MR.

Ainsi, des écueils de faisabilité restent à résoudre pour la mise en place d'une architecture type MR et ce sur les deux volets : gouvernance et gestion technique. Il faudra notamment trouver un équilibre entre rapidité de mise en place, ouverture et sécurité de l'architecture. L'adoption d'une architecture régulée repose d'abord sur la nomination d'une entité de gouvernance fédératrice (publique ou un consortium d'acteurs) en charge d'éditer des règles de gouvernance et d'audit dans le but d'authentifier les acteurs désirant intégrer l'architecture PKI.

La transition vers une architecture *Multi-Régulée.* Dans le cas où l'architecture *Multi-Régulée* serait retenue, et comme des réserves perdurent encore pour la mise en place de cette architecture dans les termes définis dans la partie 7.4, il serait préférable d'envisager une phase transitoire limitant l'action de l'autorité administrative à la gouvernance et l'édition de règles communes à la filière. Comme la situation actuelle se dirige vers une coexistence d'architectures UL non interopérables dans cette première phase la gouvernance pourrait être gérée par un consortium d'acteur régulé ou avec l'aval d'acteur de la régulation et reposerait sur des acteurs techniques existants actuellement pour assurer l'interopérabilité des systèmes. Au vu du faible nombre de Root CAs envisagés l'utilisation de *trust lists* ne paraît pas nécessaire à ce jour. En effet des solutions simples et temporaires peuvent être envisagées tel que la mise en place de plusieurs *root certificate* dans les bornes et les véhicules. Ainsi, dans un premier temps, cette autorité ne sera chargée que de la définition des règles de gouvernance minimales communes à respecter par les *V2G Root CAs* tout en détenant un pouvoir de contrôle du respect de ces règles. En parallèle, un travail de définition et de rédaction des règles de gestion de la *trust list* devra être réalisé. Une fois l'architecture ancrée et les mécanismes de gestion de la *trust list* actés, l'autorité administrative deviendra plus opérationnelle et sera en charge de la gestion de l'unique *trust list* de l'architecture PKI. Cette deuxième phase permettra d'ouvrir davantage le marché à de nouveaux *V2G Root CAs*. Cette implémentation en deux temps permettra un gain de temps significatif pour le déploiement de l'architecture type MR tout en garantissant le respect des critères définis par l'AFIREV.

Concernant les architectures UL et ML, celles-ci n'ont pas été retenues en cible pour les raisons suivantes :

- L'architecture *Unique-Libre*, bien que la plus simple et rapide à mettre en œuvre, présente de nombreux inconvénients et risques sur la transparence, l'interopérabilité et la résilience du système. N'étant ni régulé, ni concurrencé, ni audité par un acteur indépendant, le *V2G Root CA* aura la main mise sur tout le système d'opération de la certification et portera tous les risques financiers, de cybersécurité, etc. Cette architecture ne répond donc pas aux critères AFIREV.
- Concernant l'architecture *Multi-Libre*, l'introduction de la concurrence permettra d'avoir un système stable et plus résilient avec des *V2G Root CAs* potentiellement plus transparents. L'interopérabilité ne reposera donc plus sur un seul et unique acteur mais sera répartie sur un certain nombre N de *V2G Root CAs*. Cependant la mise en place de ce système repose sur la réalisation d'accord bilatéraux et l'utilisation de N *trust lists* (unique par *V2G Root CA*). Les délais nécessaires à la définition de règles communes de création et de gestion des *trust lists*, les temps de développements encore inconnus pour la mise en place de ce mécanisme et surtout l'aspect discriminatoire rendu possible par l'absence de régulation sont autant de risques qui mènent l'AFIREV à écarter cette architecture.

5. Synthèse de l'analyse sur la structuration des plateformes d'échange des certificats

5.1. Cas d'usage des plateformes de pool

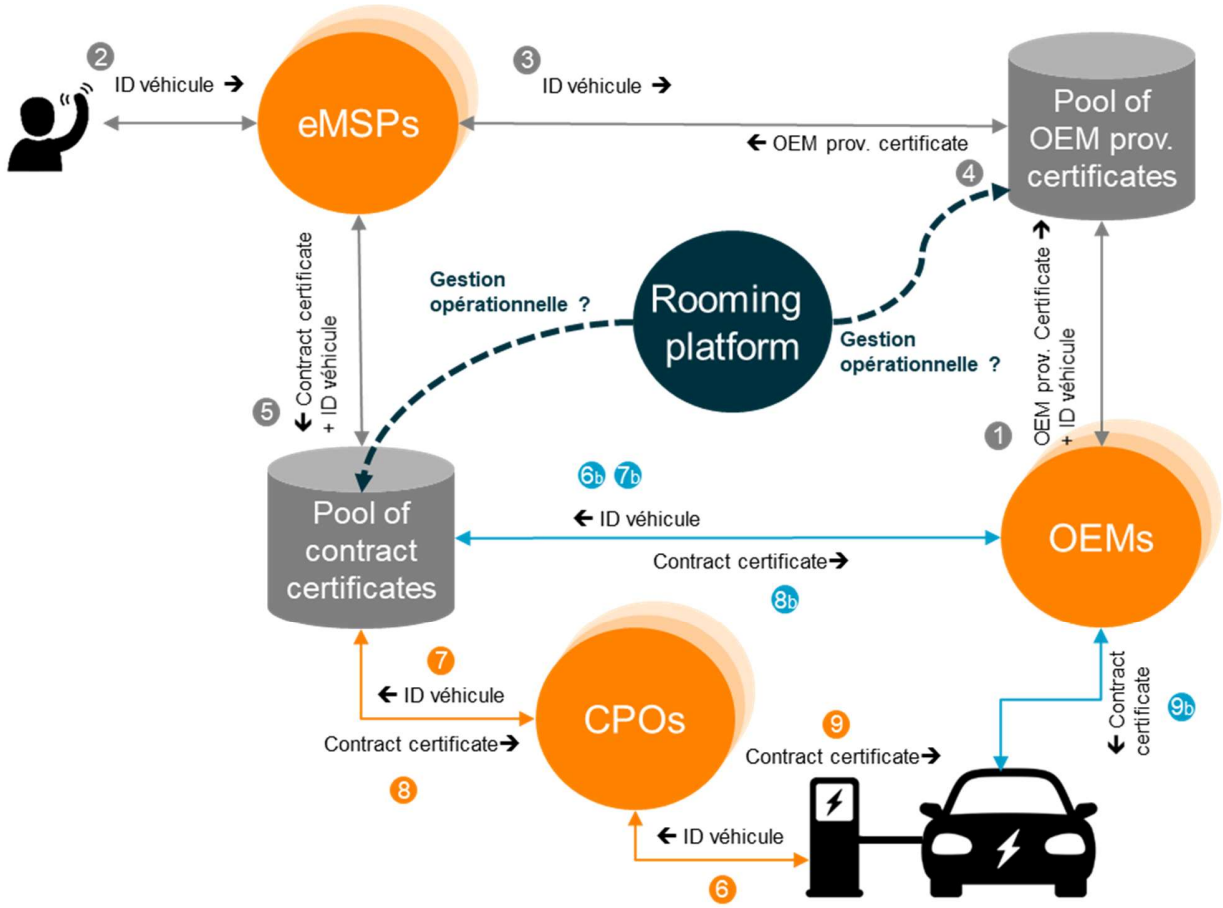

Figure 1 – Schéma de fonctionnement des pools associés à la gestion des certificats de contrat

Dans le contexte de l'ISO 15118 et de la fonction Plug and Charge, les plateformes d'échanges de certificats sont utilisées pour 3 cas d'usage majeurs : l'installation d'un certificat de contrat de mobilité dans un véhicule, la révocation de ce certificat de contrat, et le remplacement d'un certificat de contrat par un autre. Nous présentons le fonctionnement de ces plateformes de manière simplifiée afin de discuter des éventuels impacts des réflexions sur les architectures PKI sur ces plateformes.

L'installation d'un certificat de contrat de mobilité suit les étapes suivantes :

1. En amont de la remise du véhicule à son propriétaire le constructeur automobile dépose sur une plateforme d'échange le certificat *OEM provisioning certificate* associé à l'identifiant du véhicule (ID véhicule)
2. L'utilisateur du véhicule contractualise avec un opérateur de mobilité (eMSP) en lui fournissant entre autres son ID véhicule
3. A partir de cet ID véhicule l'eMSP requête la plateforme d'échange des *OEM provisioning certificate*s pour obtenir le certificat correspondant au véhicule de son nouveau client

4. Le *Pool of OEM provsioning certificate* fourni le certificat correspondant et ainsi l'eMSP peut créer un certificat de contrat de mobilité (*Contract certificate*) à partir des informations de contrat (date d'expiration, etc.), contenant son ID véhicule et le signer avec l'OEM provisioning certificate spécifiquement pour le véhicule de son client
5. L'eMSP dépose sur une plateforme d'échange le certificat *de* contrat associé à l'identifiant du véhicule (ID véhicule)

Il existe ensuite plusieurs méthodes pour installer ce certificat nous en présentons deux

6	Lors d'une première connexion à une borne ISO 15118 l'absence de *contract certificate* dans le véhicule conduit à ce que la borne requête son CPO pour en obtenir un pour le véhicule, pour cela elle lui fournit l'ID véhicule	6b - 8b	Le *Pool of contract certificates* fourni à l'OEM les *contract certificates* correspondant aux véhicules de sa fabrication à partir de leurs ID véhicules au fil de l'eau et/ou sur requête
7	Avec l'ID véhicule le CPO requête le *Pool of contract certificates*		
8	Le *Pool of contract certificates* fourni au CPO le *contract certificate* correspondant au véhicule s'il existe		
9	Le *contract certificate* correspondant au véhicule est descendu jusqu'au véhicule, via la borne, pour y être installé	9b	L'OEM installe via un lien télématique le *contract certificate* demandé par son client

D'autres méthodes d'installation peuvent être envisagée tel que la mise à jour manuelle via un support physique ou non du véhicule par son propriétaire ou un professionnel.

La révocation d'un certificat de contrat conduit un eMSP à mettre à jour le *Pool of contract certificate,* elle doit aussi être gérée au sein du véhicule pour qu'un certificat de contrat identifié comme révoqué ne soit pas stocké inutilement (désinstallation, écrasement par un autre certificat, …).

5.2. Compatibilité de la circulation des certificats avec les architectures UR et MR

Il n'existe pas d'impact du choix de l'architecture PKI sur la structuration des pools et sur leur gestion. Quel que soit l'architecture retenue il est nécessaire de mettre en place deux pools pour être en mesure de gérer les cas d'usage de création du certificat de contrat de mobilité (« contract certificate »), de son installation et de sa révocation.

La gestion, la gouvernance et les règles de marché liées à la mise en place de ces pools et à la coexistence de plusieurs gestionnaires de pools et donc de plusieurs pools pour les certificats de contrat et de plusieurs pools pour les *OEM provisioning certificate* sont des sujets qui, comme pour l'architecture de gestion PKI, restent à définir.

Pour l'AFIREV il est important de mener de front les discussions et la recherche d'un consensus à l'échelle de la plaque continentale européenne via l'UE sur le sujet des architectures PKI ISO 15118 et des pools de certificats ISO 15118 notamment sur la gestion de la gouvernance.

5.3. Gestion du chargement des certificats dans les VE

L'installation d'un certificat de contrat de mobilité dans le véhicule électrique doté de la technologie ISO 15118 Plug and Charge est une étape clef pour permettre ce service avancé de recharge.

Plusieurs canaux d'installation sont envisageables (manuel, via la borne, en concession, via la télématique), et il semble qu'un consensus se dégage chez les constructeurs automobiles pour mettre en place un processus d'installation via le lien télématique (lien de télécommunication, 3G, 4G…) entre le véhicule et un serveur de gestion côté constructeur.

Pour les constructeurs automobiles ce canal est le plus transparent pour l'expérience utilisateur car il permet une gestion des certificats digitalisée et simplifiée, hors processus de recharge, par exemple suite à la contractualisation avec un eMSP. Ce canal permet aussi une gestion de multiples contrats de mobilité et facilite grandement le changement d'eMSP (installation d'un nouveau certificat de contrat), la résiliation d'un contrat (révocation du certificat) et l'alternance entre plusieurs contrats – professionnel et personnel par exemple (interversion de certificats).

Les constructeurs automobiles souhaitent donc être connectés au gestionnaire de pool de certificat de contrat pour proposer immédiatement au client la mise à jour du contrat dans son véhicule dès qu'un nouveau certificat est disponible pour son véhicule dans le pool (mode push).

Cette solution semble être au service de l'expérience utilisateur tout en permettant une libre concurrence des eMSP sur le service de recharge Plug and Charge ISO 15118, elle doit tout de même être complétée pour apporter toutes les garanties aux acteurs de la filière sur un accès libre et équitable à l'installation de certificat de contrat dans les véhicules.

6. Recommandations AFIREV

Les travaux AFIREV menés sur les architectures PKI à déployer en premier lieu en France mais avec une vision d'intégration et d'interopérabilité en Union Européenne et sur le continent européen ont conduit aux recommandations suivantes :

> **Recommandation 1 :** L'AFIREV recommande d'initier des discussions à l'échelle européenne dans l'objectif d'élaborer un consensus en ciblant l'architecture PKI suivante : Architecture *Multi-Régulée* basée sur une autorité administrative pont.

Pour la mise en place d'une architecture type UR ou MR des règles de gouvernances communes doivent être établies.

Considérant que :

- Des acteurs ont pris des initiatives qui vont dans le sens de l'architecture MR ;
- L'architecture MR doit être définie en concertation avec les autorités Européennes, ce qui pourrait prendre un délai indéfini ;
- Une convergence avec l'organisation d'ITS doit être prévue à terme ;
- Il semble que la commission européenne ait fait le choix de l'architecture MR pour ITS (cf. 8. Annexe) ;

Il semble préférable de commencer par la mise en place de règles de gouvernance communes dans la perspective d'une organisation en architecture MR.

> **Recommandation 2 :** L'AFIREV recommande de faire émerger une maitrise d'ouvrage de l'architecture *Multi-Régulée* gérée par un regroupement d'acteurs ou une entité publique, pour la **définition de règles de gouvernance minimales communes à toute la filière** et disposant d'un pouvoir de contrôle sur le suivi de ces règles. Cette entité n'est pas nécessairement liée à l'Union Européenne dans un premier temps mais devra fédérer à l'échelle du continent à moyen termes. Cette maitrise d'ouvrage doit être collaborative afin de rassembler les multiples acteurs et consortia ayant pris position sur le sujet des PKI pour l'ISO 15118 et souhaitant voir ce sujet aboutir. Elle devra s'appuyer sur des expertises techniques sur le sujet de la gestion des PKI.

Les règles de gouvernance des deux architectures sont des éléments complexes à définir mais aussi clefs pour fédérer la filière autour d'une architecture

> **Recommandation 3 :** L'AFIREV recommande l'élaboration à l'échelle européenne de règles de gouvernance pour l'architecture PKI privilégiée (*Multi-Régulée*) qui couvrent les sujets des plateformes (pool), des règles de certification et d'audit des candidats *Sub-CA* et les exigences minimales portant sur les acteurs opérants les systèmes de certification.

La gestion technique des *trust lists* est un enjeu majeur pour réaliser l'architecture MR

> **Recommandation 4 :** L'AFIREV recommande l'étude par la filière à l'échelle européenne de spécifications techniques ainsi que de gouvernance pour la gestion des *trust list* ou des solutions techniques alternatives (cahier des charges commun à toute la filière pour l'implémentation de mécanismes de mise en place d'une trust list, des processus de sécurisation de la liste, des protocoles de transfert et de mise à jour de cette liste ainsi que d'algorithmes sécurisés de décryptage).

La gestion des plateformes de circulation des certificats (pools) et le chargement des certificats dans les véhicules sont aussi des enjeux de développement des services avancés de l'ISO 15118 tel que le Plug and Charge et de leur cyber sécurité.

> **Recommandation 5 :** L'AFIREV recommande de mener des discussions dans l'objectif d'obtenir un consensus à l'échelle de la plaque continentale européenne via l'UE sur le sujet des pools de certificats ISO 15118 notamment sur la gestion de leur gouvernance ainsi que sur le processus de chargement des certificats dans les véhicules garantissant un accès libre et équitable pour tous les EMSP.

7. Annexe : description des architectures et évaluations

7.1. Architecture UL : Une autorité unique et marchande

7.1.1. Description

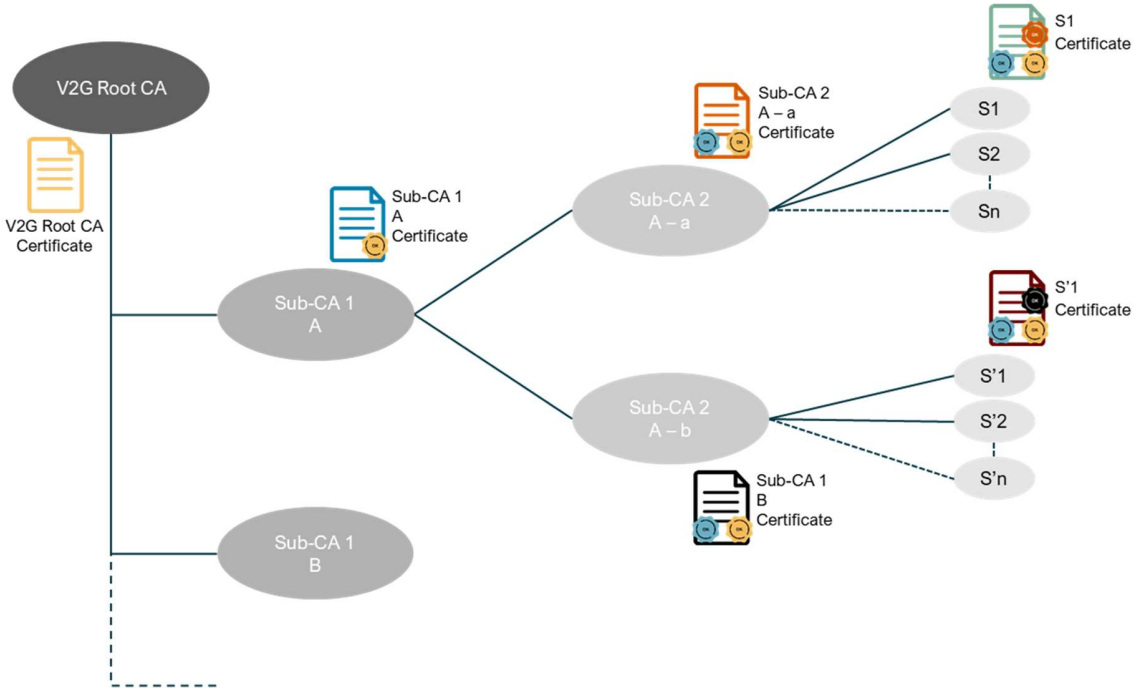

Figure 2 – Schéma fonctionnel de l'architecture UL « Une autorité unique et marchande »

Le *V2G Root CA* est un acteur économique, marchand et non régulé. Dans cette architecture, il est l'unique autorité pouvant délivrer des certificats racines (*V2G Root CA Certificates*) et donc à certifier les acteurs qui lui sont associés et ainsi permettre la sécurisation de l'architecture PKI. Tout acteur possédant le *V2G Root CA certificate* dans sa chaîne de certificats ou dans ses signatures est considéré « acteur de confiance » sur toutes les chaînes d'authentification. Le V2G Root CA procède à des audits des candidats *SubCA* et de la gestion des certificats par les acteurs qui le sollicitent.

A titre d'illustration considérons l'exemple défini en liminaire. Dans cette architecture, le *V2G Root CA* fixe des règles de gouvernance et des tarifs imposés à tout *CSO* désirant se faire certifier. Le *CSO* européen demande à être certifié contre rémunération lui accordant ainsi le droit de générer des *Sub CA Certificates* signés par le *V2G root CA*. Ce *CSO* certifie ainsi sa filiale française pour les autoroutes en lui délivrant un certificat contenant la signature du *V2G Root CA*. De cette manière, la filiale est certifiée acteur de confiance et est autorisée à générer et à installer des

certificats (*leaf certificates*) dans le parc de bornes qu'elle opère. Ces certificats dans les bornes contiennent eux aussi la signature du *V2G Root CA* assurant un lien de confiance aux véhicules qui s'y connectent.

Suite au branchement du véhicule électrique à la borne, celui-ci envoie son certificat de mobilité (*Contract Certificate*). La borne vérifie que le *V2G Root CA* a bien signé le certificat de mobilité du véhicule et qu'il correspond effectivement à celui ayant signé son *leaf certificate*. En cas de succès, un lien de confiance est donc établi entre les deux.

7.1.2. Critères d'évaluation de l'architecture UL

Critère	Evaluation sur les deux axes (interne et filière)
Nombre de V2G Root CA	1
Structure juridique du *V2G Root CA*	Entreprise privée non régulée
1. Transparence du *V2G Root CA*	**MENACE :** Le V2G Root CA fixe les **règles de gouvernance** et les applique à tous ses clients, il peut les changer selon son bon vouloir. Il n'est contraint que par les codes généraux du commerce et de la concurrence. **MENACE :** Le V2G Root CA décide de ses **tarifs** et de son **niveau de service**, il peut les modifier selon son bon vouloir. Il n'est contraint que par ses contrats signés et les codes généraux du commerce et de la concurrence. **FAIBLESSE :** L'existence d'un unique *V2G Root CA* privé est non compatible avec les règles de concurrence et règles antitrust européennes.
2. Répartition des fonctions du *V2G Root CA*	**FORCE :** Le *V2G Root CA* opère l'unique **système IT** permettant de générer des *V2G Root CA* Certificates et en établi les **règles de gouvernance**. Une cohérence et une rapidité d'exécution sont donc attendues. **MENACE :** Tous les acteurs dépendent du même *V2G Root CA* et de son système informatique. Ils n'ont aucun droit de regard. **MENACE :** Aucun **audit** du *V2G root CA* n'est possible apriori.
3. Interopérabilité du système	**FORCE :** Le système d'interopérabilité repose uniquement sur le *V2G Root CA*, et sur sa capacité à opérer la génération de certificats. La gestion de l'interopérabilité est donc simple. **OPPORTUNITE :** En cas de changement géographique d'une borne ou d'un véhicule d'une plaque d'opération d'un *V2G Root CA* vers une autre (ex : revente ou importation d'un véhicule hors Europe), il est suffisant d'installer le

	nouveau *V2G Root CA Certificate* dans le véhicule pour assurer l'interopérabilité. **MENACE :** En cas de désaccord d'un *Sub-CA*, avec le *V2G Root CA*, le système tiers n'est pas ou plus interopérable avec le reste des systèmes en contrat avec le *V2G Root CA.* **MENACE :** La position monopolistique du *V2G Root CA* risque d'engendrer un fort potentiel discriminatoire ce qui entraînerait une fragilité du système.
4. Complexité d'implémentation et de déploiement	**FORCE :** Implémentation simple du fait d'une unicité de solution et de sa gestion par un acteur et décisionnaire unique, c'est l'architecture la plus simple et certainement la plus rapide à déployer. **FORCE :** Gestion simple des règles de gouvernance du fait d'une unicité du décisionnaire. **MENACE :** Règles de gouvernance, tarifs et solution techniques pouvant évoluer sans préavis et sans droit de regard des acteurs tiers, la complexité peut être déportée chez les *Sub-CA*.
5. Existence de barrières à l'entrée pour être *V2G Root CA*	**OPPORTUNITE :** Aucune barrière à l'entrée supplémentaire, réglementaire ou technique, pour devenir *V2G root CA* **MENACE :** Cette architecture favorise l'existence d'un monopole, décourageant la création de nouveaux *V2G Root CA*.
6. Evolutivité du système	**FORCE :** L'unicité du *V2G Root CA Certificate* permet de restreindre le nombre de mise à jour, de renouvellement ou de remplacement de ce certificat. **MENACE :** L'unicité du V2G Root CA et du système IT défavorise la créativité et la prise d'initiative pour l'amélioration et la sécurisation des processus implémentés.
7. Résilience économique et technique du *V2G Root CA*	**FAIBLESSE :** En cas de faillite, plus aucune recharge n'est possible sur les bornes disposant d'un *Leaf Certificate* signé de ce *V2G Root CA*. **MENACE :** Le *V2G Root CA* peut faire faillite ou être racheté par une société tierce entraînant potentiellement la modification drastique des règles de gouvernance et des tarifs appliqués sans droit de regard des acteurs dépendant du *V2G Root CA*. **MENACE :** La compromission du *V2G root CA* est aggravée du fait de sa gouvernance non transparente (règles de communication sur les failles de sécurité auto-définies, possibilité d'audit limité etc.) **MENACE :** Une cyberattaque du système de certification causerait de lourds impacts techniques (fonctionnement

	restreint ou bloqué du système, non sécurisation des échanges en cas de non communication de la compromission du système) et financiers (investissements conséquents en cybersécurité pour pallier au défaut et pénalités). Ceci pourrait entraîner la faillite ou le rachat du *V2G Root CA*. **FORCE :** Prise de décision rapide en termes de cybersécurité du fait que le *V2G Root CA* soit un acteur centralisé.

7.2. Architecture UR : Une autorité unique régulée à l'échelle européenne/internationale

7.2.1. Description

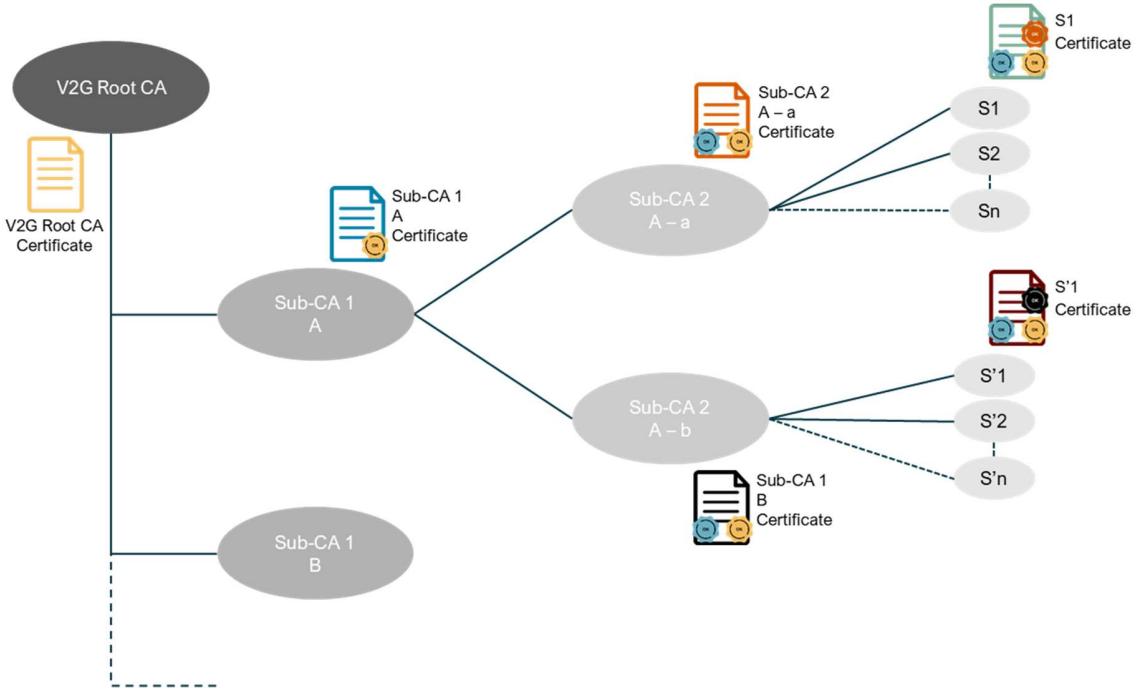

Figure 3 – Schéma fonctionnel de l'architecture UR
« Une autorité unique régulée à l'échelle Européenne ou internationale »

Le *V2G Root CA* est un acteur neutre, régulé et non marchand. Il est géré par une entité européenne ou internationale – que nous nommerons autorité régulatrice – ou par un consortium d'acteurs privés régulé par une instance européenne ou internationale qui assure la mise en place de règles non discriminatoires pour l'adhésion au consortium – nous le nommerons consortium régulé. Ce *V2G Root CA* (autorité régulatrice ou consortium régulé) se porte garant du bon fonctionnement de l'architecture et de la transparence des règles de gouvernance et des règles tarifaires. Ce *V2G Root CA* est considéré par toute la filière comme l'unique autorité pouvant délivrer des certificats racines (*V2G Root CA Certificates*) et donc à certifier les acteurs qui lui sont associés et ainsi permettre la sécurisation de l'architecture PKI. Tout acteur possédant le *V2G Root CA Certificate* est considéré « acteur de confiance » sur toutes les chaînes d'authentification.

Ce *V2G Root CA* peut être une autorité purement administrative sans compétences techniques requises pour gérer la certification et sous-traiter la gestion du système informatique de signature de certificats et l'audit des acteurs à certifier (*Sub-CA 1*) à des acteurs tiers par le biais d'appels d'offres. Tous les répondants peuvent, lors du processus de sélection du prestataire, être auditer par une entité indépendante et missionnée par l'autorité régulatrice. Pour résumer, trois fonctions apparaissent :

- Définition des règles de gouvernance et de tarifs : gérée par l'autorité de gouvernance (autorité régulatrice ou consortium régulé) qui fixe des règles de gouvernance clairement établies et partagées. Concernant les tarifs ceux-ci peuvent être définis à priori ou à posteriori des appels d'offres ; ils restent néanmoins fixes et connus par tous les acteurs concernés de la chaîne,
- Gestion du système de certification : gérée par l'autorité de gouvernance si elle dispose des compétences nécessaires ou par un prestataire extérieur après un appel d'offres. Dans ce deuxième cas, le prestataire est en charge du maintien en condition opérationnelle du système tandis que l'autorité de gouvernance se porte garant du bon fonctionnement de la chaîne de certification,
- Audit des candidats *Sub-CA* et de la gestion des certificats : gérée par l'autorité de gouvernance si elle dispose des compétences nécessaires ou confié à un organisme spécialisé indépendant en charge entre autres de vérifier la capacité du répondant à opérer le système de certification, et d'auditer les candidats à la certification *Sub-CA dans* le respect des règles imposées par l'autorité de gouvernance dans son cahier des charges. L'audit du *V2G Root CA* – « Gestionnaire du système de certification » peut être rendue publique dans un souci de transparence.

A titre d'illustration nous allons considérer l'exemple défini en liminaire. Dans cette architecture, le *V2G Root CA* – « Autorité de gouvernance » fixe des règles de gouvernance, définit les tarifs en vigueur et les met à disposition de tout *CSO* désirant se faire certifier. Suite à deux appels d'offres il sélectionne un *V2G Root CA* – « Auditeur » et un *V2G Root CA* – « Gestionnaire du système de certification » qu'il contrôle régulièrement afin d'assurer un bon niveau de service.

Le *CSO* européen demande à être certifié. Après audit par le *V2G Root CA* – « Auditeur », le *V2G Root CA* – « Gestionnaire du système de certification » certifie le *CSO* lui accordant ainsi le droit de générer des *Sub CA Certificates* signés par le *V2G root CA*. Ce *CSO* certifie ainsi sa filiale française pour les autoroutes en lui délivrant un certificat contenant la signature du *V2G Root CA*. De cette manière, la filiale est certifiée acteur de confiance et est autorisée à générer et installer des certificats (*leaf certificates*) dans le parc de borne qu'elle opère. Ces certificats dans les bornes contiennent eux aussi la signature du *V2G Root CA* assurant un lien de confiance aux véhicules qui s'y connectent.

Suite au branchement du véhicule électrique à la borne, celui-ci envoie son certificat de mobilité (*Contract Certificate*). La borne vérifie que le *V2G Root CA* a bien signé le certificat de mobilité du véhicule et qu'il correspond effectivement à celui ayant signé son *leaf certificate*. En cas de succès, un lien de confiance est donc établi entre les deux.

7.2.2. Critères d'évaluation de l'architecture UR

Critère	Evaluation sur les deux axes (interne et filière)
Nombre de *V2G Root CA*	1
Structure juridique du *V2G Root CA*	Entité neutre et régulée (entreprise, association, organisme)
1. Transparence du *V2G Root CA*	**FORCE :** Les **règles de gouvernance** sont établies et évoluent au travers de la régulation et sont donc connues de tous. Les acteurs dépendant du *V2G root CA* ont connaissance de ces règles et peuvent même contribuer à leur mise en place ou leur évaluation. **FORCE :** Le **tarif** de certification du *V2G Root CA* est régulé et connu par les différents acteurs.
2. Répartition des fonctions du *V2G Root CA*	**FORCE :** Une séparation peut être mise en place entre les différentes fonctions du *V2G Root CA* : • Gouvernance par une autorité indépendante • Gestion opérationnelle de la génération de certificats gérés par un acteur tiers IT • Audit des acteurs (gestionnaire du système IT et Sub-CA 1) par un acteur spécialisé
3. Interopérabilité du système	**FORCE :** Le système d'interopérabilité repose uniquement sur le *V2G Root CA*, et de sa capacité à opérer la génération de certificats **FORCE :** L'existence d'une autorité administrative non marchande permet de fédérer la filière **OPPORTUNITE :** C'est une autorité administrative indépendante et régulée qui est garante de l'interopérabilité de la sécurité de communication ce qui limiterait l'émergence de multiple V2G root CA « privatifs »
4. Complexité d'implémentation et de déploiement	**FORCE :** Implémentation simple du fait d'une unicité de solution et de sa gestion par un acteur et décisionnaire unique. Au niveau technique, cette architecture est simple à déployer. **FAIBLESSE :** C'est une architecture complexe car elle ne dépend pas nécessairement d'un seul et unique acteur et elle passe par une forme de régulation qui peut être longue à mettre en place. **MENACE :** En cas de remplacement contraint du *V2G Root CA* – « Gestionnaire du système de certification », les délais de mise en place de l'appel d'offre et d'appropriation ou de

	modification du système IT peuvent entraîner des disfonctionnements et une baisse de qualité du système.
5. Existence de barrières à l'entrée pour être *V2G Root CA*	**OPPORTUNITE :** La régulation privilégie un unique *V2G root CA* pour la gouvernance ce qui limite fortement la possibilité pour un nouvel acteur de s'établir comme *V2G root CA*. **OPPORTUNITE :** La gestion opérationnelle de la génération de certificats peut être gérée par un acteur tiers IT au travers d'appels d'offres. **OPPORTUNITE :** La mise en place d'un *V2G Root CA* – « Auditeur » permet d'assurer un suivi de la qualité de service du gestionnaire du système IT.
6. Evolutivité du système	**FORCE :** La clé privée permettant la certification des acteurs reste la propriété de l'autorité de gouvernance et n'est pas dépendante d'un acteur économique. **FAIBLESSE :** Possibilité de compromission de l'architecture si la clé privée est découverte par le gestionnaire du système de certification. **MENACE :** L'unicité du V2G Root CA et du système IT défavorise la créativité et la prise d'initiative pour l'amélioration et la sécurisation des processus implémentés.
7. Résilience économique et technique du *V2G Root CA*	**FORCE :** La potentielle séparation des rôles du *V2G root CA*, et la nature non économique de l'autorité de gouvernance rend cette architecture plus résiliente face à la disparition de l'opérateur de certification ou de l'opérateur d'audit. **FORCE :** La potentielle séparation des rôles du *V2G root CA*, et la nature non économique de l'autorité de gouvernance rend cette architecture transparente face à la compromission de l'opérateur de certification et il lui est plus facile de faire évoluer son niveau de sécurité ou de le récupérer après compromission. **FORCE :** Afin d'assurer une cybersécurisation du système, des critères de cybersécurité peuvent être intégrés de manière transparente dans le cahier des charges lors de l'émission de l'appel d'offre pour la gestion du système IT de certification.

7.3. Architecture ML : Une fédération de certifications croisées

7.3.1. Description

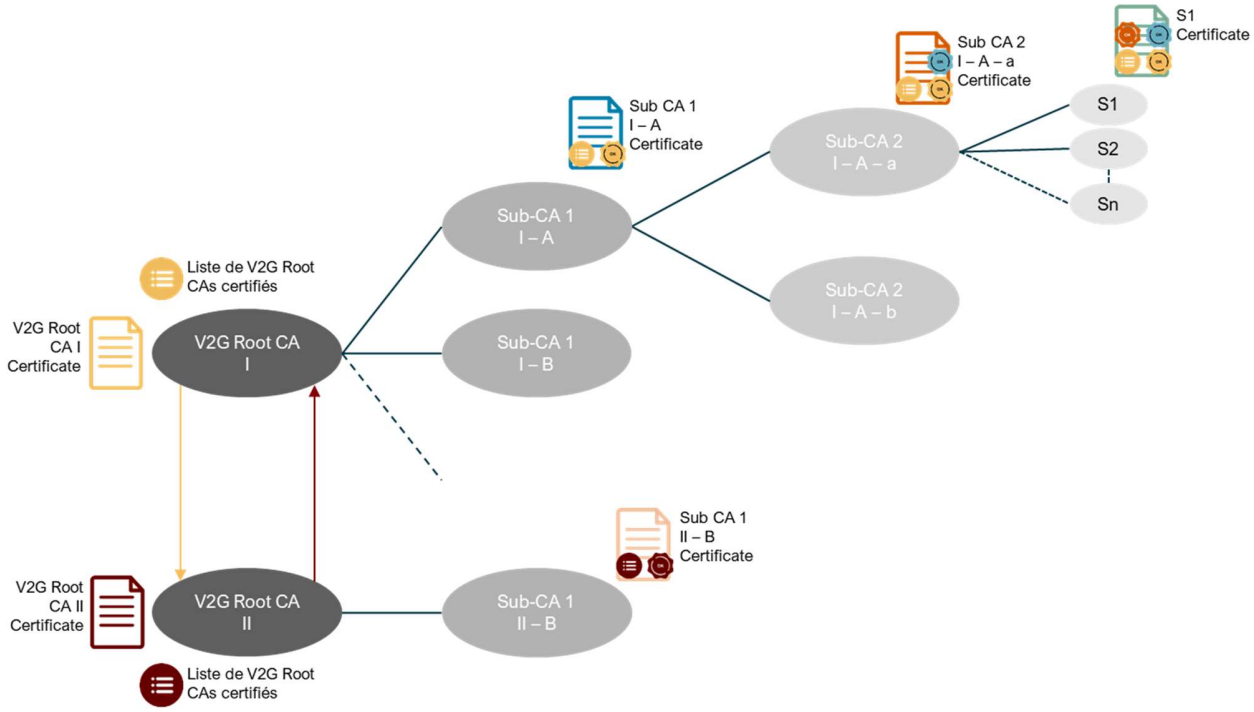

Figure 4 – Schéma fonctionnel de l'architecture ML « Une fédération de certifications croisées »

Dans cette architecture, il n'existe pas un mais plusieurs *V2G Root CAs* qui coexistent et dont la structure juridique n'est pas imposée. Ils peuvent être par exemple des autorités régulées, des entreprises marchandes, des consortiums et regroupement d'entreprises ou même des organismes privés ou publiques. Chaque *V2G Root CA* gère sa propre chaîne de certification de manière comparable aux architectures UL ou UR : chaque *V2G Root CA* définit ses propres règles de gouvernance et ses propres tarifs. Cependant un lien bilatéral entre *V2G Root CAs* est nécessaire afin d'assurer l'interopérabilité du système. Chaque nouvel entrant désirant offrir un service de V2G Root CA devra réaliser des certifications croisées avec tous les *V2G Root CAs* déjà en place (ou à minima ceux gérant la zone géographique l'intéressant).

Considérons l'exemple décrit dans le liminaire avec un *V2G Root CA* fonctionnant sur le principe de l'architecture UL (i.e. un acteur économique, marchand et non régulé) et un deuxième *V2G Root CA* fonctionnant sur le principe de l'architecture UR (i.e. un acteur neutre, régulé et non marchand dont le SI est géré par un prestataire externe et audité). Lors de l'établissement du lien contractuel entre les deux *V2G Root CAs,* chaque *V2G Root CA* met à jour[14] sa propre et unique liste de V2G Root CAs de confiance (*trust list*) et la transmet aux acteurs sous son autorité. Cette liste peut être intégrée au *V2G Root CA Certificate, ou sinon transmise parallèlement à celui-ci*.

[14] Le mécanisme de gestion des *trust lists* n'est pas spécifié dans l'ISO 15118. Le processus de transfert, de sécurisation, de mise à jour et de déchiffrage des *trust lists* reste à définir pour le PnC.

Les *V2G Root CAs* listés sont ainsi considérés comme des sous autorités et leur certification est considérée valide. L'interopérabilité des systèmes est assurée comme l'explique les exemples ci-après.

Lors de la certification du *CSO* européen par son *V2G Root CA*, puis de la filiale française des autoroutes et voies rapide par sa maison mère puis des bornes par la filiale, les *trust lists* sont intégrées et partagées dans les certificats transitant entre les différents paliers. Ainsi chaque borne a à sa disposition la signature de son *V2G Root CA* « officiel » ainsi que la *trust list* contenant tous les autres *V2G Root CAs* acceptés.

Suite au branchement du véhicule électrique à la borne, celui-ci envoie son certificat de mobilité (*Contract Certificate*). La borne vérifie que ce contrat est bien signé par le *V2G Root CA* officiel ayant signé son *leaf certificate* ou à défaut par un *V2G Root CA* renseigné sur la *trust list* à sa disposition. En cas de succès, un lien de confiance est donc établi entre les deux.

Il est à noter que chaque *trust list* est unique et est associée à un seul et unique *V2G Root CA* qui la signe ; il existe donc autant de *trust lists* que de *V2G Root CAs* et par conséquent tout autant de combinaisons possibles.

7.3.2. Critères d'évaluation de l'architecture ML

Critère	Evaluation sur les deux axes (interne et filière)
Nombre de *V2G Root CA*	N
Structure juridique du *V2G Root CA*	Plusieurs entités de structures juridiques différentes peuvent coexister (autorité neutre et régulée, entreprise marchande, association, organisme publique ou privé)
1. Transparence du *V2G Root CA*	**FORCE :** Les règles de gouvernance sont propres à chaque *V2G Root CA*. **FORCE :** Chaque *Sub-CA 1* dispose d'un large panel de *V2G Root CA* afin de choisir les règles de gouvernance et les tarifs qui lui conviennent. **FAIBLESSE :** Absence de transparence sur les règles de gouvernances des *V2G Root CAs*. **FAIBLESSE :** Absence de transparence tarifaires ; chaque *V2G Root CA* fixe ses propres tarifs et règles tarifaires. **OPPORTUNITE :** La mise en concurrence des *V2G Root CAs* permettra une homogénéisation des règles de gouvernance, des tarifs et des règles tarifaires.
2. Répartition des fonctions du *V2G Root CA*	**FORCE :** Chaque *V2G Root CA* est libre de choisir son système de fonctionnement. **FAIBLESSE :** L'audit des *V2G Root CAs* n'est pas obligatoire. **OPPORTUNITE :** La mise en concurrence des *V2G Root CAs* permettra une homogénéisation des règles d'audit des *V2G Root CAs* et des *Sub-CA 1*.
3. Interopérabilité du système	**FORCE :** Au sein d'une même architecture, l'interopérabilité est totale. L'utilisation de *trust lists* permet d'étendre cette interopérabilité à d'autres acteurs mais **FAIBLESSE :** la multiplicité des *trust lists* peut être une contrainte à une interopérabilité complète du système. **FAIBLESSE :** La taille des *trust lists* augmente en fonction du nombre de *V2G Root CAs* interopérables. La mise à jour de ces *trust list* peut rapidement devenir un facteur limitant du déploiement d'un système interopérable. **FAIBLESSE :** Les processus d'interprétation des *trust lists* ne sont pas définit dans l'ISO 15118. L'interopérabilité ne peut fonctionner (au niveau européen et mondial) sans convergence des algorithmes de lecture des *trust lists* (respectivement au niveau européen et mondial).

4. Complexité d'implémentation et de déploiement	**FAIBLESSE :** Le déploiement de cette architecture peut être complexifié et retardé par la prise en compte, la formalisation et le développement de protocoles de création, de distribution, de mise à jour et d'interprétation des *trust lists*. **FAIBLESSE :** Le maintien en condition opérationnelle du système peut être entravé par une complexité technique lié à la multiplicité des accords d'interopérabilité.
5. Existence de barrières à l'entrée pour être *V2G Root CA*	**OPPORTUNITE :** Tout nouvel acteur peut se déclarer *V2G Root CA*. **FAIBLESSE :** Pour des raisons de sécurité, la mise à jour des *trust lists* doit se faire à une fréquence définit. Les risques de brèches de sécurité augmentent avec la fréquence de mise à jour. Un délai d'attente est à considérer pour tout nouveau *V2G Root CA* désirant intégrer une *trust list*. **MENACE :** Cette architecture favorisera le ou les *V2G Root CAs* capables de mettre en place une architecture PKI dans des délais très courts et ainsi de capter rapidement un maximum de *Sub-CAs 1*.
6. Evolutivité du système	**FAIBLESSE :** L'interopérabilité des systèmes passent par des accords bilatéraux entre *V2G Root CAs*. La fréquence et la disparité des mises à jour des *trust lists* pourraient introduire des risques de cybersécurité.
7. Résilience économique et technique du *V2G Root CA*	**FORCE :** En cas de **chute** d'un *V2G Root CA*, les autres continuent d'opérer leur système en restant interopérables entre eux. **FORCE :** En cas de **compromission** d'un *V2G Root CA*, celui-ci est retiré de la *trust list* de tous les autres *V2G Root CAs* avec un accord bilatéral qui continuent d'opérer leur système en restant interopérables entre eux. **MENACE :** Les règles de communication sur les failles de sécurité étant auto-définies par chaque *V2G Root CA*, la **compromission** unilatérale de tous les systèmes IT est aggravée.

7.4. Architecture MR : Une autorité administrative pont

7.4.1. Description

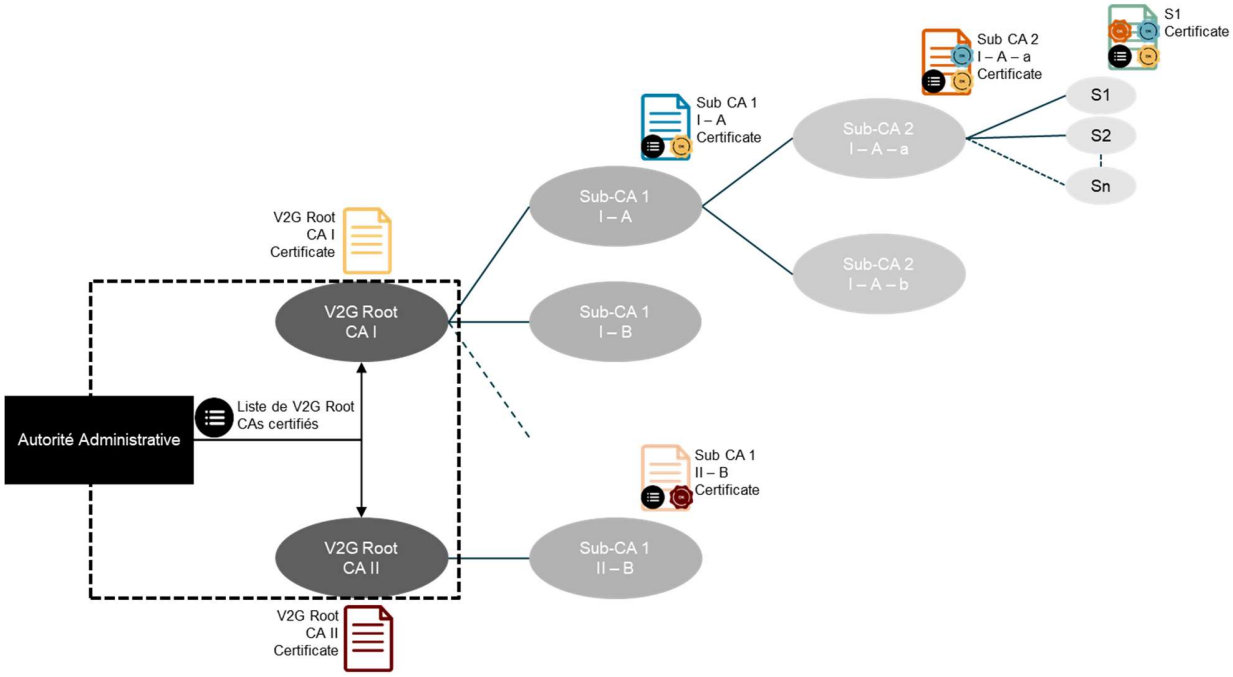

Figure 5 – Schéma fonctionnel de l'architecture MR « Une autorité administrative pont »

Cette architecture est comparable à l'architecture C à la différence près que la liste des *V2G Root CAs* certifiés (*trust list*) est gérée et tenue à jour[15] par une autorité administrative indépendante et neutre sans compétences techniques requises pour gérer la certification. De plus, cette *trust list* est unique et commune à tous les *V2G Root CAs* qui y sont inscrits. Dans cette architecture, l'autorité administrative fixe des règles de gouvernance minimales (RGM) applicables à tout *V2G Root CA* désirant intégrer la *trust list* et de ce fait être interopérable avec tous les *V2G Root CAs* déjà rattachés à l'autorité administrative. Cette autorité a aussi la possibilité de contractualiser suite à un appel d'offres avec un cabinet d'audit spécialisé pour certifier et suivre le respect des RGM par les *V2G Root CAs*. L'audit des Sub-CA 1 restant à la main de chaque *V2G Root CAs*.

Chaque nouvel entrant désirant offrir un service d'interopérabilité à ses clients devra se rapprocher de l'autorité administrative qui, après audit et vérification du respect des règles de gouvernance minimales, mettra à jour la *trust list* en y ajoutant ce nouvel entrant. Cette liste sera ensuite transmise à tous les *V2G Root CAs* qui y sont inscrits et qui sont chargés d'en informer les acteurs dépendant de leur architecture. Ce fonctionnement permet de réduire le besoin de co-certification entre les *V2G Root CAs* ce qui simplifie les démarches nécessaires pour avoir un système à la fois sécurisé et interopérable.

[15] Le mécanisme de gestion des *trust lists* n'est pas spécifié dans l'ISO 15118. Le processus de transfert, de sécurisation, de mise à jour et de déchiffrage des *trust lists* reste à définir pour le PnC.

A titre d'exemple, considérons le cas d'usage décrit dans le liminaire avec de plus une autorité administrative européenne. Considérons ici trois *V2G Root CAs* de structures juridiques différentes que nous nommerons *V2G Root CA 1*, *V2G Root CA 2* et *V2G Root CA 3*. De plus supposons que le *V2G Root CA 3* est déjà inscrit sur la *trust list*.

Afin de rendre leurs systèmes interopérables à grande échelle, les deux *V2G Root CAs* (1 et 2) se rapprochent de l'autorité administrative pour demander l'adhésion à la *trust list*. Celle-ci démarre un processus d'audit pour vérifier que ses règles de gouvernances (RGM) sont bien respectées par chaque *V2G Root CA*.

Trois cas d'usages sont possibles :

- Le *V2G Root CA 1* ne respecte pas les règles de gouvernances minimales : il n'est pas intégré à la liste. Ce *V2G Root CA* ne pourra pas accéder au service d'interopérabilité via l'autorité administrative et est invité à renouveler sa demande après amélioration de ses règles de gouvernances,
- Le *V2G Root CA 2* respecte les règles de gouvernances minimales : il intègre la *trust list* qui est mise à jour et transmise à tous les acteurs s'y trouvant. Ce *V2G Root CA* pourra donc proposer un service d'interopérabilité à ses clients via l'autorité administrative,
- Le *V2G Root CA 3*, *déjà inscrit sur la trust list*, est compromis, fait faillite ou ne respecte plus les règles de gouvernances minimales imposées par l'autorité administrative : il est donc retiré de la *trust list*. Celle-ci est mise à jour et tous les « acteurs de confiance » en sont informés. le *V2G Root CA 3* ne pourra plus accéder au service d'interopérabilité via l'autorité administrative.

Avec la transmission de la *trust list* aux *V2G Root CAs* rattachés à l'autorité administrative, les *V2G Root CAs* listés sont considérés comme des sous autorités et leur certification est considérée valide. C'est ainsi que fonctionnera l'interopérabilité des systèmes.

Lors de la certification du *CSO* européen par son *V2G Root CA*, puis de la filiale française des autoroutes et voies rapide par sa maison mère puis des bornes par la filiale, les *trust lists* sont intégrées et partagées dans les certificats transitant entre les différents paliers. Ainsi chaque borne a à sa disposition la signature de son *V2G Root CA* « officiel » ainsi que la *trust list* contenant tous les autres *V2G Root CAs* acceptés.

Suite au branchement du véhicule électrique à la borne, celui-ci envoie son certificat de mobilité (*Contract Certificate*). La borne vérifie que ce contrat est bien signé par le V2G Root CA officiel ayant signé son *leaf certificate* ou à défaut par un *V2G Root CA* renseigné sur la trust list à sa disposition. En cas de succès, un lien de confiance est donc établi entre les deux.

7.4.2. Critères d'évaluation de l'architecture MR

Critère	Evaluation sur les deux axes (interne et filière)
Nombre de *V2G Root CA*	N
Structure juridique du *V2G Root CA*	Plusieurs entités de structures différentes peuvent coexister (autorité neutre et régulée, entreprise marchande, association, organisme publique ou privé)
1. *Transparence du V2G Root CA*	**FORCE :** Mise en place par une autorité administrative de règles de gouvernances minimales à respecter par tous les *V2G Root CAs* désirant avoir un système interopérable via le système de *trust list*. **FORCE :** Les règles de gouvernance sont propres à chaque *V2G Root CA*. **FORCE :** Chaque *Sub-CA 1* dispose d'un large panel de *V2G Root CA* afin de choisir les règles de gouvernance qui lui conviennent. **FAIBLESSE :** Multiplication des complexités de gouvernance à cause des 2 échelles (autorité administrative et *V2G Root CA*). **FAIBLESSE :** Absence de transparence sur les règles de gouvernances des *V2G Root CAs*. **FAIBLESSE :** Absence de transparence tarifaires ; chaque *V2G Root CA* fixe ses propres tarifs et règles tarifaires **OPPORTUNITE :** La mise en concurrence des *V2G Root CAs* permettra une homogénéisation des règles de gouvernance, des tarifs et des règles tarifaires.
2. Répartition des fonctions du *V2G Root CA*	**FORCE :** Chaque *V2G Root CA* opère son système permettant de générer des *V2G Root CA Certificates* et en établi les règles de gouvernance. **FORCE :** L'autorité administrative audite les *V2G Root CAs* et n'intègre dans la *trust list* que ceux respectant des règles de gouvernance minimales. **OPPORTUNITE :** La mise en concurrence des *V2G Root CAs* permettra une homogénéisation des règles d'audit des *V2G Root CAs* et des *Sub-CA 1*.
3. Interopérabilité du système	**FORCE :** L'interopérabilité est gérée par une autorité neutre, la co-certification mutuelle entre V2G Root CAs n'est plus nécessaire pour le fonctionnement de l'itinérance. **OPPORTUNITE :** Possibilité d'intégrer à tout moment de nouveaux *V2G Root CAs* de confiance grâce à la neutralité de l'autorité administrative et au processus d'acceptation.

	OPPORTUNITE : La *trust list* permet de rendre interopérables des architectures préexistantes non interopérables sans en changer fondamentalement la structure. Il suffit de mettre à jour la *trust list*. **MENACE :** Encourage à la multiplication des *V2G Root CAs* ce qui pourrait générer des complexités dans la gestion de l'itinérance.
4. Complexité d'implémentation et de déploiement	**FAIBLESSE :** Le déploiement de cette architecture peut être complexifié et retardé par la prise en compte, la formalisation et le développement de protocoles de création, de distribution, de mise à jour et d'interprétation de la *trust list*. **FAIBLESSE :** Le maintien en condition opérationnelle du système peut être entravé par une complexité technique lié à la multiplicité des demandes d'accords d'interopérabilité. **MENACE :** Encourage à la multiplication des *V2G Root CAs* (des règles de gouvernances différentes, des systèmes informatiques différents, une *trust list* de plus en plus lourde à maintenir à jour régulièrement).
5. Existence de barrières à l'entrée pour être *V2G Root CA*	**OPPORTUNITE :** Tout nouvel acteur peut se déclarer *V2G Root CA*. **FAIBLESSE :** Pour des raisons de sécurité, la mise à jour de la *trust list* doit se faire à une fréquence définit. Les risques de brèches de sécurité augmentent avec la fréquence de mise à jour. Un délai d'attente est à considérer pour tout nouveau *V2G Root CA* désirant intégrer une *trust list*.
6. Evolutivité du système	**FAIBLESSE :** L'interopérabilité des systèmes passent par une mise à jour de la *trust list* au niveau des systèmes IT de tous les *V2G Root CAs* renseignés. La fréquence et la disparité des mises à jour des *trust lists* pourraient introduire des risques de cybersécurité.
7. Résilience économique et technique du *V2G Root CA*	**FORCE :** En cas de **chute** d'un V2G Root, les autres continuent d'opérer leur système en restant interopérables entre eux mais **FAIBLESSE :** une mise à jour de la *trust list* est nécessaire. **FORCE :** En cas de **compromission** d'un V2G Root, les autres continuent d'opérer leur système en restant interopérables entre eux mais **FAIBLESSE :** une mise à jour de la *trust list* est nécessaire. **MENACE :** Les règles de communication sur les failles de sécurité étant auto-définies par chaque *V2G Root CA*, la **compromission** d'un ou plusieurs les systèmes IT est aggravée.

8. Annexe : Exemple d'architecture MR mise en place pour le véhicule connecté C-ITS

Dans l'objectif de déployer progressivement l'interopérabilité de communication entre véhicules (V2V), avec pour objectif de débuter une phase d'industrialisation avant fin 2020 la Commission Européenne s'est constituée comme autorité de gouvernance de la solution C-ITS V2X. Elle est à disposition des acteurs désirant faire partie de la phase de test et d'industrialisation qui évoluera vers la mise en place de *Root CA* (RCA) indépendants. L'acceptabilité de la solution C-ITS V2X est déjà forte et certains constructeurs automobiles tel que Volkswagen déploient dès aujourd'hui cette solution dans leurs modèles. Il est à noter que cette phase de test est entièrement financée par la CE

Afin de donner un cadre et une gouvernance clair au déploiement de la solution, une architecture PKI de type *Multi-Régulée* a été instaurée par la CE. La CE est *C-ITS certificate policy authority*. Elle édite une *Certificate policy*, en tant que *Certificate Policy Authority* (CPA), qui définit les règles de gouvernance et d'organisation des entités certifiées. A ce titre elle approuve ou rejette les candidatures de *Root CA* sur la base notamment d'audits. Le *Root CA* peut être privé ou public, sans limitation de nombre si ce n'est un problème de d'alourdissement de la Trust List et donc de temps de traitement.

La Trust List est un fichier statique fréquemment mis à jour et régulièrement téléchargé par tous les objets liés à l'architecture PKI. Cette unique liste est disponible sur le site du CPOC

Dans ce cadre, celle-ci a émis un appel d'offre pour l'implémentation d'une solution de Trust List Manager (TLM) respectant des spécifications techniques et de gouvernances rédigées par l'ETSI. Cette solution implémentée par Thalès est actuellement gérée directement par la CE qui peut révoquer un Root CA de la *European Certificate Trust List.*

D'autre part, dans l'architecture PKI utilisée par la CE, un C-ITS Point Of Contact est utilisé comme interface utilisateur permettant aux différentes entités rattachées à l'architecture d'accéder à l'ECTL (European Certificate Trust List), plus communément appelée *Trust List* (TL). Celui-ci étant indépendant du TLM). Le TLM et C-ITS Point of Contact sont sous le contrôle de la CE mais il peut être envisagé qu'ils puissent être sous le contrôle de deux entités séparées.

Le Root CA certifie deux autorités :

- Une autorité d'enrôlement (EA) : émet les certificats d'enrôlement / d'identification de la voiture. Ce certificat, de durée de vie limitée, est délivré en cours de vie du véhicule et non en sortie d'usine. Ils permettent de signer les messages envoyés en wifi ou en 5G par le véhicule et reçus par les véhicules voisins. Afin d'empêcher de retracer l'historique de déplacement d'un véhicule, le certificat pseudonyme utilisé pour la signature du message change régulièrement. Chaque véhicule dispose de plusieurs certificats pseudonymes (environ une centaine par semaine).
- Une autorité d'autorisation (AA) : émet les certificats d'autorisation, c'est-à-dire les certificats détaillant les messages spécifiques à l'usage du véhicule pouvant être envoyé (« Je suis prioritaire » pour les ambulances / véhicules de pompiers / gendarmerie …, « Je tourne à droite » pour tous les véhicules, « Je passe au rouge » pour les feux tricolores…).
- L'EA et l'AA doivent être opérés séparément pour éviter la traçabilité d'un véhicule.

Le CPA (*Certificate Policy Authority*), autorité politique des certificats, est l'autorité responsable de la mise en place de politiques de gestion des certificats et de celle de gestion des autorisations PKI. Cette autorité est composée d'acteurs publics et privés.

Avant de figurer dans la TL, chaque *Root CAs* doit réaliser une procédure de déclaration au CPA, cette procédure se déroule en ligne et en physique entre les représentants de chaque partie (Cette procédure est à refaire pour tout renouvellement de certificat) :

- Afin de valider la véracité des documents envoyés en ligne, le système d'identifiants eID (*Electronic Identification*) / eIDAS (*Electronic Identification Authentification and trust Services)* est utilisé par C-ITS pour la signature des documents avant leur envoie.
- Pour la phase en physique, un représentant du Root CA (*RCA AR – Root CA Authorized Representative*) doit se rendre physiquement à la CPA pour s'authentifier et présenter son dossier. Le CPOC *Authorized Representative* vérifie si les spécifications précisées dans le dossier sont réellement à la portée du Root CA.
- Un audit de la conformité du CPS (*Certification Policy Statement*) par rapport au CP (Certificat Policy) édité par le CPA est réalisé par un auditeur accrédité choisi par la CE.
- Une fois validé par le CPA et le CPOC, le certificat du Root CA est transmis au TLM puis ajouté à la Trust List.

Contact

Gilles Bernard

gilles.bernard@afirev.fr

22 Avenue Jean AICARD, 75011 Paris, France