UNIVERSITÉ DU QUÉBEC

MÉMOIRE PRÉSENTÉ À
L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES

COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN MATHÉMATIQUES ET INFORMATIQUE
APPLIQUÉES

PAR
ABDERRAHMANE SADALI

DÉVELOPPEMENT D'UNE INFRASTRUCTURE À CLÉS PUBLIQUES POUR LES RÉSEAUX V2G MULTI DOMAINES

SEPTEMBER 2023

Résumé

Étant donné que les véhicules électriques devraient gagner en popularité dans un proche avenir, un déploiement à grande échelle de l'infrastructure Vehicle To Grid (V2G) est prévu. Il permettrait de couvrir de grandes régions géographiques telles que des pays et des continents. Il s'agira donc d'un réseau complexe qui nécessitera plusieurs domaines administratifs et qui impliquera plusieurs organisations propriétaires.

À cet égard, un cadre de confiance approprié est nécessaire pour permettre aux véhicules électriques et aux bornes de recharge d'assurer la fourniture d'informations et de services fiables. D'où la nécessité d'une Public key infrastructure (PKI) *globale, robuste* et *évolutive qui soit définies selon les normes par l'ISO 15118*.

L'infrastructure PKI offre une structure de confiance entre ses utilisateurs, ou mandants. Cependant, son déploiement pose des problèmes importants, car de nombreux pays et entreprises peuvent utiliser divers systèmes et règles de sécurité. Ceci pose la question de l'interopérabilité entre ces différentes implémentations.

Dans ce mémoire, nous proposons une solution basée sur une infrastructure PKI inter-domaine qui offre une couverture globale sur un réseau V2G en assurant les propriétés les plus fondamentales de la sécurité. Avec l'utilisation de l'outil de modélisation formelle Tamarin Prover et le simulateur RISE — V2G, nous avons pu démontrer la validité et l'efficacité de notre proposition.

Abstract

Since electric vehicles are expected to gain popularity in the near future. A large-scale deployment of V2G infrastructure is expected, which will certainly span large geographic regions such as countries and continents, so it will be a complex network that will require multiple administrative domains and involve multiple owner organizations.

In this regard, an appropriate trust framework is needed to enable electric vehicle and charging station to ensure the provision of reliable information and services. Consequently, the demand for a *worldwide*, *resilient*, *and scalable* Public Key Infrastructure (PKI) aligns harmoniously with the ISO 15118 standard, cementing its significance.

PKI offers a structure of trust between its users, or principals. However, there are significant problems with PKI deployment because many countries and companies may use various security systems and rules. This raises the question of interoperation between these various implementations.

In this thesis, we propose a solution based on inter-domain PKI infrastructure that provides a global coverage on a V2G network while ensuring the most fundamentals properties of security. Using the formal modelling tool Tamarin Prover and the RISE-V2G simulator, we were able to demonstrate the validity and efficacy of our proposal.

Remerciement

Je remercie Dieu, le tout puissant, pour m'avoir donné le courage, la patience, la volonté et la force nécessaire pour affronter toutes les difficultés et les obstacles qui se sont hissés au travers de mon chemin d'étude.

La rédaction de ce mémoire a été possible grâce au concours de plusieurs personnes à qui je voudrais témoigner toute ma gratitude.

Je voudrais en premier temps remercier, mon professeur, mon directeur de mémoire, Boucif Amar Bensaber, pour sa patience, sa disponibilité et surtout ses judicieux conseils qui ont contribué à alimenter ma réflexion.

J'adresse mes sincères remerciements à tous les professeurs et chercheurs qui, par leurs paroles, leurs écrits, leurs conseils et leurs critiques, ont guidé mes réflexions et ont accepté de me rencontrer et de répondre à mes questions durant mes recherches.

Je remercie les professeurs Ismail Biskri et Mhamed Mesfioui d'avoir accepté d'évaluer ce travail.

Je désire remercier l'équipe pédagogique du département de mathématique et informatique de l'Université du Québec à Trois-Rivières qui m'ont fourni les outils nécessaires à la réussite de mes études universitaires.

Je voudrais exprimer ma reconnaissance envers les amis et collègues qui m'ont apporté leur soutien moral et intellectuel tout au long de ma démarche.

Enfin, je remercie ma famille, leur soutien inconditionnel et leurs encouragements ont été d'une grande aide. Je remercie mes très chers parents qui ont toujours été là pour moi. Je remercie mes sœurs et mon frère pour leur encouragement.

À tous, je présente mes remerciements, mon respect et ma gratitude.

Table des matières

Liste des tableaux

Table des figures

Liste des abréviations

CO2 Carbon dioxide

V2G Vehicle To Grid

EVCC Electric vehicle communication controler

SECC Suply equipment communication controler

EV Electric Vehicle

EMSP Electric mobility service provider

OEM Original Equipment Manufacturer

PnC plug and change

EIM External Identification Means

PKI Public Key Infrastructure

ECDSA Elliptic Curve Digital Signature Algorithm

DES Data Encryption Standard

AES Advanced Encryption Standard

SHA Secure Hash Algorithm

CA Certification authority

NSSEC Non Super Singular Elliptic Curve.

Chapitre I

1. Introduction

Les inquiétudes concernant le réchauffement climatique et l'indépendance énergétique se répandent dans le monde entier. La dépendance importante à l'égard de ressources étrangères pour assouvir cette « dépendance au pétrole » ainsi que la compréhension croissante des effets des émissions de Carbon dioxyde (CO2) sur le réchauffement climatique sont des forces majeures qui poussent vers le développement de nouvelles technologies de transport. En améliorant l'efficacité énergétique et en utilisant des sources d'énergie alternatives vertes, ces technologies cherchent à réduire considérablement l'empreinte carbone.

Ces problèmes sont pris en charge notamment par le développement de voitures hybrides rechargeables ou 100 % électriques. Les constructeurs automobiles créent actuellement de nouveaux produits après avoir entendu l'appel au développement de nouvelles voitures. Ce qui explique d'où provient le concept de l'exigence d'une batterie qui fournit toute l'énergie nécessaire ou une partie de celle-ci à la propulsion d'un véhicule électrique (VE).

Le niveau de tension de distribution est utilisé pour intégrer les VE dans le réseau en raison de leur nature et de leurs propriétés physiques. Chaque VE peut désormais être connecté au réseau pour obtenir la puissance nécessaire à la recharge de sa batterie. Les VE représentent une nouvelle charge que l'infrastructure énergétique doit fournir. Pourtant, étant donné que les transferts de l'énergie bidirectionnels sont possibles à la suite de la mise en place de l'interconnexion, la batterie du VE peut être bien plus qu'une simple source d'énergie. En fait, la connexion permet le déploiement du VE en tant que ressource pour la production et le stockage d'énergie pendant des périodes déterminées. Un tel déploiement aide l'opérateur du système à maintenir des opérations fiables de manière plus rentable.

Ce flux d'énergie bidirectionnel entre le VE et le réseau électrique est désigné par le terme « Vehicle to Grid (V2G) », qui explique l'idée de déployer les VE en tant que ressources distribuées en les intégrant dans le réseau comme des dispositifs de charge et de génération/stockage.

Selon cette théorie, les VE participent activement aux opérations du réseau et ont un impact significatif sur l'amélioration des caractéristiques économiques et environnementales du système.

Ces avantages sont dans la fourniture de services supplémentaires basés sur l'énergie et la capacité d'élimination de l'exigence de pointes et le nivellement de la charge.

Avec ces avantages qui améliorent bien l'économie et l'environnement, les VE ont gagné en popularité. Ainsi, pour les prochaines années, un important déploiement de VE est à prévoir en tant que moyen de réduire les émissions de dioxyde de carbone (CO_2) et d'encourager l'utilisation de sources d'énergie renouvelable intermittente en se servant de systèmes de stockage d'énergie. En 2012, seulement 120 000 VE ont été vendus dans le monde. Mais avec les avantages mentionnés précédemment, pour l'année 2021, ce sont plus de 120 000 VE qui furent vendus chaque semaine. Ce qui est équivalent à près de 10 % des ventes mondiales de voitures en 2021 [1].

Le nombre de VE dans le monde en décembre 2022 a monté à 19 000 000. Ces VE préviennent l'émission de plus de 150 millions de tonnes métriques de CO_2 [2]. Actuellement, au Québec, les enregistrements de VE se chiffrent désormais à 170 592, soit une progression de 41 993 seulement en 2022, une progression de 32,65 %, correspondant à un ajout net de 41 993 VE sur les routes du Québec (Voir Fig.1). En comparaison, il y avait approximativement 39 % de croissance lors des deux années précédentes [2].

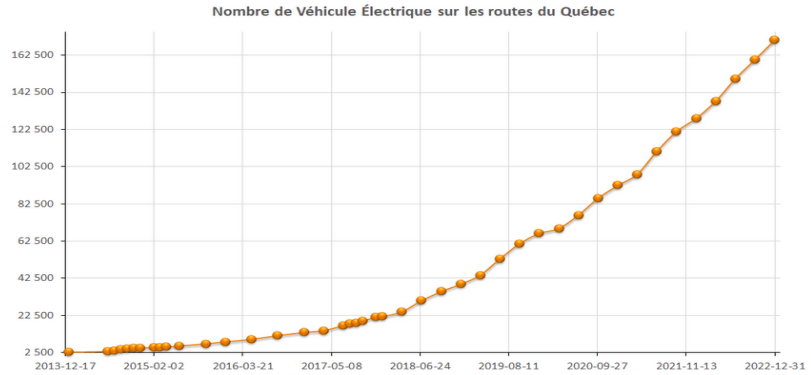

Figure 1 Croissance du nombre de Véhicules électriques sur les routes du Québec [2]

L'introduction de nombreux véhicules risque d'être difficile à gérer et pourrait entrainer des problèmes de capacité des infrastructures. Les concepteurs de VE ont proposé le réseau V2G pour l'échange des informations et de l'énergie entre les véhicules et les bornes de recharge. Ce réseau utilise les technologies de l'information et de la communication pour améliorer les performances globales des véhicules électriques et des bornes de recharge [3]. Cela permet d'échanger, entre autres, la quantité d'électricité nécessaire, les tarifs, les informations des véhicules et la disponibilité de l'électricité.

De plus, avec une telle croissance, le processus de communication et d'échange d'informations entre le VE et la borne nécessitera des exigences de sécurité pour garantir l'échange d'informations et de services sécurisés et fiables.
Ces informations peuvent inclure des éléments tels que l'identité du propriétaire, l'immatriculation de la voiture, sa capacité énergétique, les informations sur le véhicule, les cartes bancaires et les contrats entre le gestionnaire de l'infrastructure électrique et le VE. Ces données sont toutes menacées par la cybercriminalité.

Un certain nombre de solutions ont été proposées dans la littérature pour minimiser les attaques en ligne. Ces solutions incluent la préservation de l'anonymat et le secret des entités ainsi que la confidentialité, l'intégrité et la non-répudiation des informations transférées entre les automobiles et les bornes de recharge. Cependant, quand on parle des préventions des cyber-attaques, on ne peut pas oublier l'authentification des entités dans les échanges V2G. Le processus d'authentification permet de vérifier l'identité d'une entité et d'autoriser l'accès de cette entité à ses ressources et ainsi d'empêcher l'accès des entités illégales.

Dans le processus d'authentification par nom réel, les données privées des véhicules seront divulguées si certaines informations délicates (par exemple, l'identité du véhicule) sont envoyées à la borne en texte clair. Les véhicules peuvent même être suivis illégalement en utilisant les informations extraites illicitement. La technologie d'authentification anonyme de l'identité peut permettre de vérifier l'identité légale des utilisateurs sans révéler d'informations délicates. De ce fait, l'authentification anonyme occupe une place critique dans la sécurité informatique et est devenue l'une des principales orientations des chercheurs [4].

La communication dans le réseau V2G entre le VE et la borne est standardisée par la norme internationale ISO 15118 [5]. C'est une norme internationale qui décrit le protocole de communication numérique que le VE et la borne de recharge doivent utiliser lors du processus de chargement/déchargement de la batterie. Afin de protéger les échanges entre les entités sur le réseau V2G, ce standard a recommandé l'utilisation de l'infrastructure d'échange de clés publiques PKI X.509 [6]. Toutefois, à travers la documentation, il était critiqué par plusieurs chercheurs quant à la longueur du chemin de certification et le type de certificat utilisé. De plus, il ne prend pas en charge l'infrastructure PKI inter-domaine [6] et l'authentification anonyme n'est pas non plus requise. [4]

Dans le cadre de ce travail de recherche, nous allons proposer un protocole qui améliore et étend le standard ISO15118 par le support de la PKI inter-domaines tout en intégrant l'authentification anonyme. Dans la suite de ce mémoire, le chapitre 2 présente le réseau V2G d'un point de vue global en présentant les acteurs du réseau ainsi que les enjeux sécuritaires auxquels le réseau V2G fait face. Le chapitre 3 consiste en une revue des travaux réalisés dans le domaine. Dans le chapitre 4, nous proposons notre modèle avec la méthodologie utilisée et la cinématique des échanges des informations. Ensuite, nous présentons au chapitre 5 l'environnement de simulation utilisé pour nos différents tests. Les résultats obtenus au cours de nos simulations seront présentés au chapitre 6. Enfin, au chapitre 7, nous présentons une conclusion générale et les perspectives de développement futures.

Chapitre II

Généralités sur le réseau V2G et sa sécurité

2.1. Introduction

Dans ce chapitre, nous allons présenter le réseau V2G ainsi que ses composants et son infrastructure selon le modèle ISO15118. Il sera également question de l'historique de la première version ISO15118 qui fut publiée originalement il y a 10 ans pour être modifiée et enrichie à plusieurs reprises. Ensuite, nous allons spécifier en relief les implications sécuritaires liées au V2G.

2.2. Le réseau V2G

Ce réseau représente un concept permettant aux véhicules électriques d'agir comme une forme de stockage d'énergie distribué en fournissant des services de réponse à la demande du réseau électrique. Les batteries des véhicules en stationnement peuvent donc être utilisées pour faire circuler l'électricité de la voiture vers le réseau de distribution et vice-versa. Ce concept technique repose sur l'idée d'utiliser les batteries des voitures électriques en stationnement dans les deux sens. D'un côté, elle absorbe et stocke l'électricité produite en excès sur le réseau et de l'autre, elle constitue une réserve d'électricité alimentant le grand réseau ou un réseau domestique en cas de besoins. (Voir Fig.2)

Figure 2 Technologie Vehicle To Grid

La technologie V2G intervient dans le contexte où elle voit la batterie d'un VE comme une extension du réseau électrique et une réserve d'énergie dans laquelle les fournisseurs d'électricité peuvent puiser à l'occasion. La charge devient alors un processus bidirectionnel. C'est-à-dire que le réseau n'est plus utilisé uniquement pour alimenter la batterie du véhicule, mais la batterie est également utilisée comme une source d'énergie utiliser pour répondre à divers besoins de consommation d'énergie.

2.3. Infrastructure du réseau V2G

Afin de comprendre ce concept qui consiste à absorber et à donner l'énergie à partir du véhicule, il faut connaitre et comprendre les composants et l'architecture de cette technologie. Il y a deux parties majeures dans cette technologie. (Voir Fig.3).

- Le VE qui a comme composantes principales :
  - Contrôleur de communication d'équipement de véhicule (EVCC) : c'est un composant qui établit une passerelle pour échanger des informations et des données de charge entre le VE et la borne de recharge électrique. Cela a lieu entre l'Équipement d'alimentation de véhicules électriques (EVSE) et l'Electronique Control unit (ECU).
  - Système de gestion de la batterie (BMS) : c'est un système utilisé pour surveiller et contrôler les systèmes de stockage d'énergie. Il assure aussi la santé des cellules de la batterie et fournit de l'énergie aux systèmes du véhicule.
- La borne de charge qui a pour composantes :
  - Contrôleur de communication des équipements d'approvisionnement (SECC) : ce contrôleur sert comme une interface de communication entre un ou plusieurs EVCC où il peut communiquer avec les acteurs secondaires.
  - Compteur d'énergie électrique : c'est un équipement de mesure de l'énergie électrique.

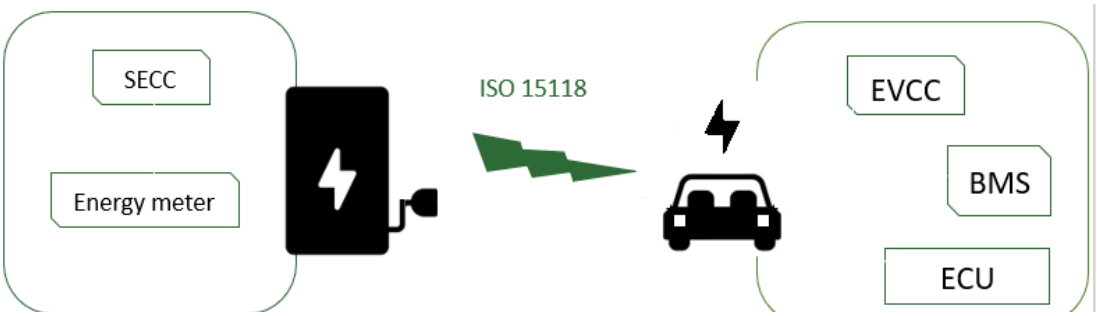

Figure 3 Infrastructure V2G

2.4. ISO 15118

ISO 15118 représente une norme internationale qui décrit le protocole de communication que le VE et la borne de charge doivent utiliser pour recharger la batterie. Cette norme couvre tous les cas d'utilisation liés à la charge à travers le monde. Cela inclut les applications de recharge filaires (courant alternatif et courant continu, AC et DC), ainsi que les pantographes utilisés pour recharger des véhicules plus volumineux comme les autobus.

Elle permet également un transfert d'énergie bidirectionnel afin de réaliser des applications véhicule-réseau en réinjectant l'énergie du VE dans le réseau en cas de besoin. La norme ISO 15118 permet aussi d'effectuer une séance de recharge des VE plus adaptée au réseau, plus sûre et plus pratique.

La première version de ISO15118 est née en 2013. Elle est divisée en 8 parties listées ci-dessous selon leur date de publication (Voir Fig.4) :

Partie 1 : Concepts de base du réseau V2G et cas d'utilisation (avril 2013).

Partie 2 : Exigences de base des couches 3 et 7 du modèle OSI (mars 2014).

Partie 3 : Exigences de base de la couche physique et de la couche liaison de données du modèle OSI (mai 2015).

Partie 4 : Tests de conformité des protocoles réseau et application (mai 2018).

Partie 5 : Tests de conformité de la couche physique et de la couche liaison de données du modèle OSI (mai 2018).

Partie 8 : Exigences des couches physiques et accès aux données pour la communication sans fil (mai 2018).

Partie 20 : Deuxième génération de la partie exigences relatives aux réseaux et aux protocoles d'application (2020).

Partie 9 : Tests de conformité de la couche physique Wifi et d'accès aux données (novembre 2022).

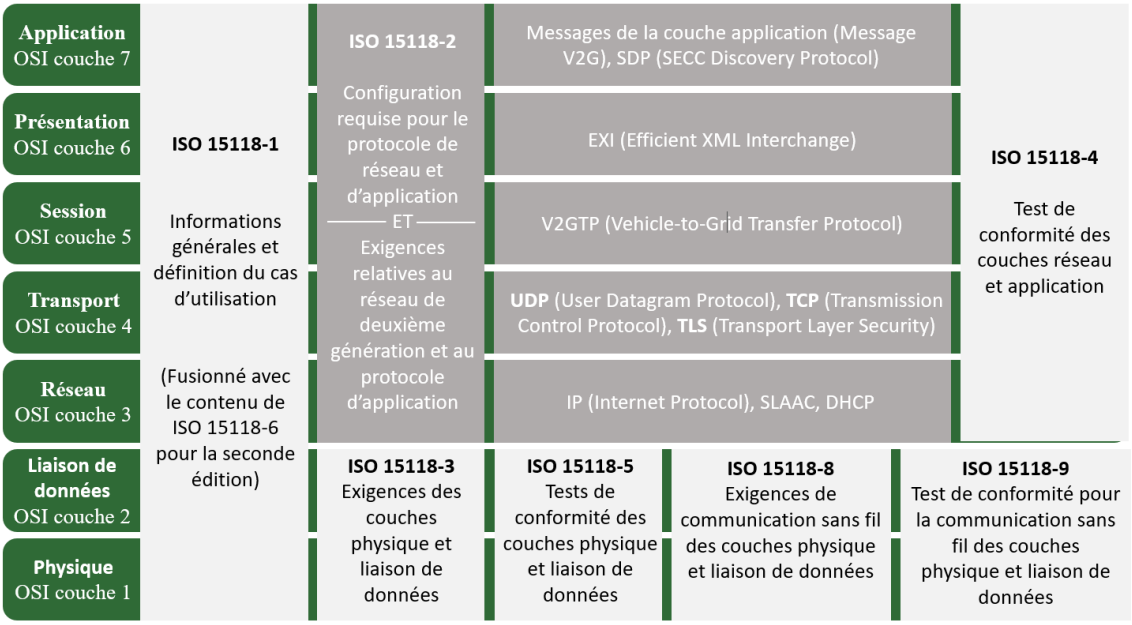

Figure 4 Parties ISO15118 dans la littérature

2.4.1. Les acteurs principaux

Un acteur principal évoque une entité qui caractérise un rôle joué par un utilisateur ou tout autre système qui interagisse avec le sujet. Le VE et l'EVSE caractérisent les acteurs principaux du modèle ISO15118. (Voir Fig.5)

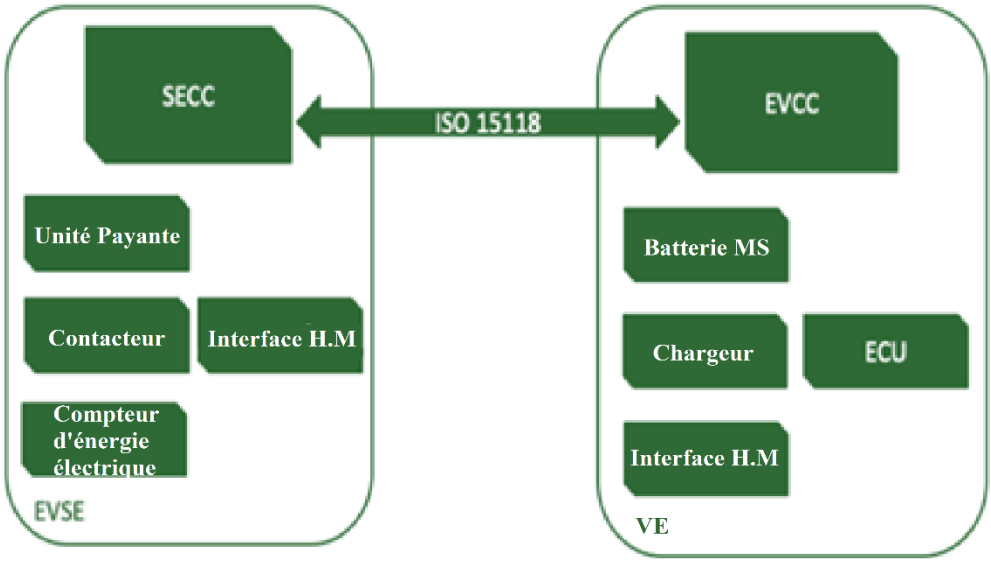

Figure 5 Acteurs principaux et leurs composant selon ISO15118

2.4.2. Les acteurs secondaires

Un acteur secondaire évoque une entité impliquée indirectement dans le processus de facturation. Selon ISO15118, les acteurs secondaires peuvent échanger des informations entre eux. On peut citer : les opérateurs mobile, fabricants d'équipement d'origine, etc. (Voir Fig.6)

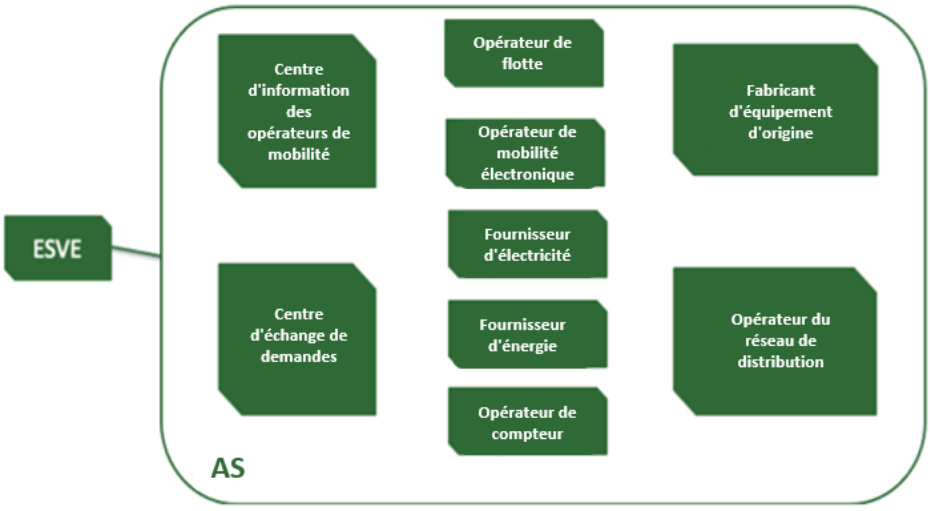

Figure 6 Acteurs secondaires selon ISO15118

2.5. La sécurité des réseaux V2G

Pour répondre aux besoins du processus de chargement du VE dans les systèmes V2G, la communication d'informations entre le VE et la borne devient cruciale. Il faut empêcher les cybers attaquants d'intercepter les communications produites entre les deux parties. Les identités de la borne et du VE doivent être sécurisées tout au long du contact afin de protéger la confidentialité de la communication des données entre eux.

Les besoins de chargement du VE peuvent ne pas être satisfaits si la borne de recharge détecte ces besoins de manière incorrecte ou si elle reçoit des informations de chargement inexactes d'une source malveillante.

Comme tout système informatique, le réseau V2G est confronté à plusieurs types d'attaques. Au nombre de ces attaques, on peut citer :

- *Le déni de service :* consiste à rendre indisponible une ressource matérielle ou logicielle aux clients par la surcharge du réseau en requêtes.

- *L'attaque de l'homme du milieu :* représente un type d'écoute clandestine dans laquelle un tiers observe et/ou altère la communication entre deux utilisateurs. Les deux parties autorisées semblent communiquer régulièrement tout au long du processus. L'émetteur de la communication ignore que le malfaiteur tente d'accéder ou de modifier le message avant de le retransmettre au récepteur.
- *L'usurpation d'identité :* une entité usurpe l'identité d'une autre, elle se fait passer par une borne de recharge ou un véhicule électrique.
- *L'attaque par rebond :* signifie une attaque contre un VE ou une borne de recharge par l'intermédiaire d'une autre entité afin de masquer ses traces.

2.6. Mesures de sécurité

Le système de chargement des VE connecte les véhicules au réseau électrique et à un système de gestion des paiements ainsi qu'à divers fournisseurs de services. L'écosystème du VE est conçu pour envoyer et recevoir des données. Il doit fournir un module de sécurité qui sécurise la communication entre le véhicule et la borne afin de protéger l'authentification de l'utilisateur et le processus de paiement. Les mesures de sécurité qui doivent être prises en compte sont :

- *Confidentialité :* les données (l'objet et les acteurs) de la communication ne doivent pas être connues par un tiers non autorisé.
  - Solutions : Cryptage, contrôle d'accès.

- *Intégrité :* représente une clause qui traite de la sécurité des modifications de données non approuvées. Le système doit être en mesure de reconnaître les cas de tentative de manipulation de données par des parties non autorisées, y compris l'ajout, la suppression et le remplacement de données réelles par d'autres afin de garantir l'intégrité de celles-ci.
  - Solutions : Mot de passe, carte à puce, empreinte digitale, signature numérique.

- *Authenticité :* l'identité des acteurs de la communication est vérifiée.
  - Solutions : Cryptage, signature numérique, contrôle d'accès, contrôle d'intégrité.

- *Non-Répudiation :* la répudiation définit le comportement d'une entité qui nie malhonnêtement avoir reçu ou envoyé certaines informations au cours d'une transaction ou d'une communication au travers d'un réseau.
  - Solution : Signature numérique.
- *Disponibilité :* s'assurer que l'information et les services soient accessibles lorsqu'ils sont demandés.
  - Solutions : Sauvegardes, partage de charge.

- *Anonymat :* il importe que toutes les parties concernées restent anonymes afin de dissimuler le lien entre les données transférées et son propriétaire. Cela pourrait rendre inutiles les données interceptées par un attaquant potentiel en cas d'attaque.
  - Solution : Pseudo entité.

2.7. Mécanismes de sécurité

2.7.1. Cryptographie

La cryptologie, qui inclut la cryptanalyse et la cryptographie, concerne l'étude des méthodes de communication sécurisées. La confidentialité et/ou la validité d'un message sont destinées à être protégées par les processus de chiffrement et de déchiffrement utilisés en cryptographie, un sous-domaine de la cryptologie. La cryptographie est considérée comme une science qui maintient la sécurité d'un message plutôt que d'uniquement se référer à la fourniture de la sécurité de l'information.

2.7.3. Cryptographie symétrique et asymétrique

Une clé est requise pour les opérations de chiffrement et de déchiffrement afin de protéger le secret du fonctionnement interne de l'algorithme. Les méthodes de chiffrement basées sur des clés peuvent être divisées en deux catégories :

- *Algorithmes symétriques :* consiste en un algorithme dans lequel les clés de chiffrement et de déchiffrement demeurent identiques. Cette formule est également connue sous le nom de formule à clé secrète ou formule à clé unique.
- *Algorithme asymétrique :* utilise une clé distincte, la clé publique, pour le chiffrement et une clé privée pour le déchiffrement.

2.7.4. Hachage

Il existe un processus mathématique connu sous le nom d'algorithme de hachage. Celui-ci brouille les données et les rend inintelligibles. Comme les techniques de hachage utilisent des programmes à sens unique, personne d'autre ne peut décoder ou déballer leur contenu. Cela parvient à prouver que les données n'ont pas été modifiées ou révisées après la fin de l'utilisation par l'auteur.

2.7.5. Signature numérique

La signature numérique consiste en une technique mathématique de pointe utilisée pour vérifier l'intégrité et la validité des messages et documents numériques. Cette technique aide à contrer le problème de l'usurpation d'identité et de la falsification dans les communications numériques. De plus, elle garantit que le contenu d'un message n'est pas modifié pendant son transit.

2.7.6. Certificat numérique

Le certificat numérique, également nommé certificat de clé publique ou propriété d'une clé publique, se lie cryptographiquement à l'entité qui la possède. Les clés publiques utilisées pour l'authentification et le chiffrement sont partagées par des certificats numériques. En plus de la clé publique qui est certifiée, les certificats numériques contiennent également des métadonnées, une signature

numérique de la clé publique émise par l'émetteur du certificat, ainsi que des informations sur l'entité qui détient la clé publique.

2.7.8. Blockchain (chaine de blocs)

Théoriquement, une blockchain ou chaine de blocs est considéré comme une structure de données distribuée permettant d'horodater les communications. Les chaines de blocs facilitent la création d'un réseau de pairs dispersé où les participants non fiables peuvent interagir de manière vérifiable sans avoir besoin d'un tiers fiable. Pour ce faire, on pourrait penser à la chaine de blocs comme un ensemble de mécanismes interconnectés qui donnent à l'infrastructure ses qualités. [7]

2.8. Infrastructure à clé publique

L'infrastructure à clé publique (PKI), initialement présentée en 1976 [8], est qualifiée comme une architecture complète de sécurité de l'information permettant de fournir des données et des communications sécurisées sur un réseau précis. L'utilisation et la nécessité de cette infrastructure augmentent continuellement. Elle fut créée pour prendre en charge la cryptographie à clé publique. Avec ce type de chiffrement, l'expéditeur chiffrera le message à l'aide de la clé publique du destinataire et seul le destinataire pourra le déchiffrer à l'aide de la clé privée correspondante.

2.8.1. Primitives de PKI

2.8.1.1. Clé publique et privée.

Les termes clé publique et clé privée sont employés largement en cryptographie. Elles comportent une utilisation différente l'une de l'autre, soit pour chiffrer et pour déchiffrer les données. Malgré leur différence, ces clés restent mathématiquement liées. Comme leur nom l'indique, la première représente la clé publique et la seconde représente la clé privée. Celles-ci se complètent et sont ainsi produites par paires.

2.8.1.2. Les certificats X.509

En conjonction avec la norme X.500, les certificats X.509 furent initialement publiés en 1988 [9]. Elles relient la valeur d'une clé publique à l'identité de la personne, de l'appareil ou du service qui possède la clé privée correspondante par une déclaration signée numériquement.

2.8.1.3. Autorité de certification (AC)

L'autorité de certification (AC) porte également le nom d'émetteur de certificats. L'AC est utilisé pour créer à la fois des listes de révocation et des certificats. Chaque certificat est livré à une entité précise en portant la signature numérique de l'autorité de certification émettrice. Chaque certificat peut être révoqué pour un certain nombre de raisons, notamment la perte de la clé privée, la compromission de la clé ou l'expiration du certificat.

2.8.1.4. Autorité d'enregistrement (AR)

L'autorité d'enregistrement (AR) est utilisée pour soumettre toutes les demandes à l'autorité de certification. De ce fait, elle confirme l'identité de tous les utilisateurs et enregistre les données de l'utilisateur final avant la certification. Si l'autorité d'enregistrement valide la requête, la demande de certificat passera directement à l'autorité de certification.

2.8.1.5. Systèmes de distribution et référentiel de certificats

Le système de distribution et le système de référentiel de certificats agissent telle une base de données pour une autorité de certification où les certificats numériques sont stockés. Ils sont utilisés comme mécanisme de stockage assurant le suivi des certificats et de la liste de révocation de certificats.

2.8.2. Architectures de PKI

2.8.2.1. Architecture hiérarchique

Avec une architecture hiérarchique, il existe un seul certificat autosigné qui appartient à l'autorité de certification racine. Cette autorité se signe avec sa propre clé privée. Les interactions de confiance sont unidirectionnelles et tous les

utilisateurs font confiance à la même AC racine. De plus, comme le canal de certificat est unidirectionnel, la conception et la validation des chemins de certificat deviennent simples. (Voir Fig. 7) :

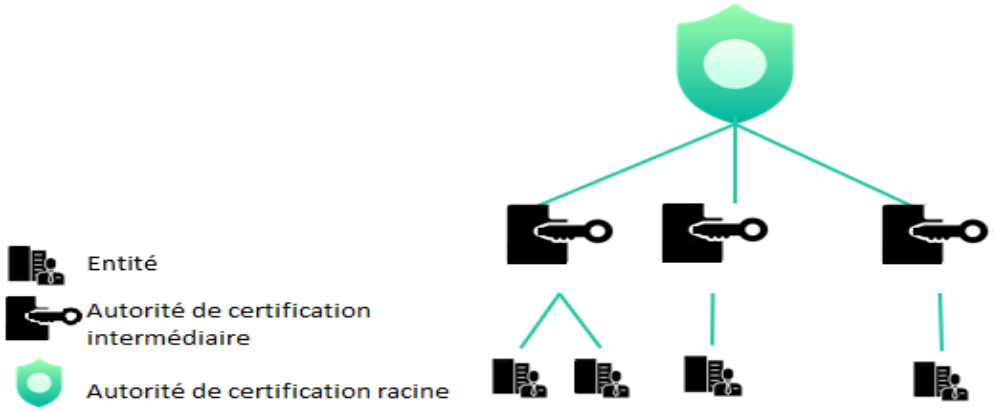

Figure 7 Architecture hiérarchique

2.8.2.2. Architecture Peer to Peer

Cette approche se constitue d'une série de modèles homologues où chaque AC effectue une certification croisée avec toutes les autres autorités de certification. Les autorités de certification locale d'un utilisateur servent d'ancre de confiance. Les AC, dans cet environnement, n'ont pas de relation supérieure et la compromission d'une seule autorité de certification ne peut pas faire tomber l'ensemble de l'infrastructure à clé publique. [10] (Voir Fig. 8) :

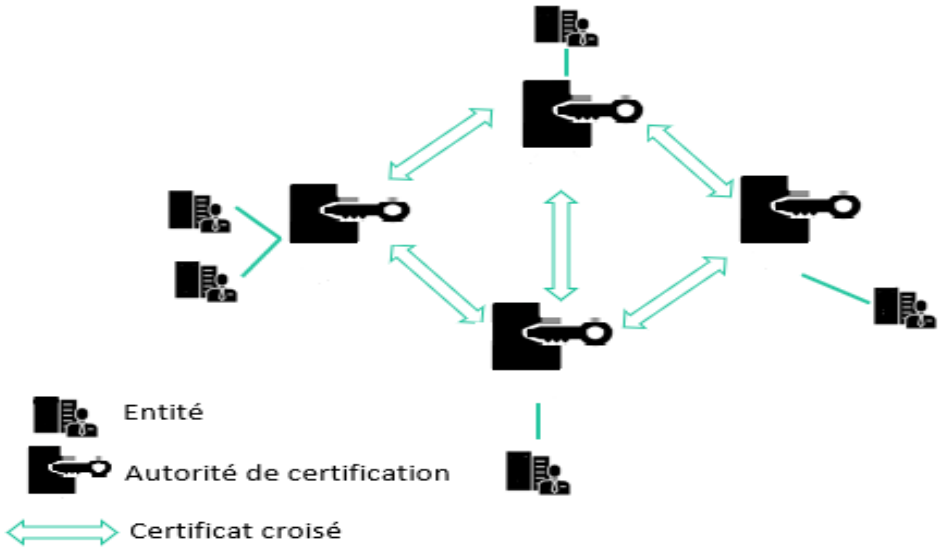

Figure 8 Architecture Peer to Peer

2.8.2.3. Architecture du pont

Cette architecture a été conçue pour combler les lacunes de l'architecture hiérarchique et de l'architecture Peer to Peer [10]. Dans ce concept, un "Bridge CA" est utilisé pour relier deux PKI hiérarchiques. En s'accordant des certificats croisés, l'AC Racine 1 et l'AC de pont sont liées. En ce sens, l'AC 2 et l'AC de pont sont liées de la même manière. Les applications doivent uniquement faire confiance au certificat Bridge CA pour traiter les certificats de l'une des deux PKI. Lorsque l'autorité de certification Bridge est ajoutée à l'ancre de confiance locale, la confiance est automatiquement formée. (Voir Fig. 9) :

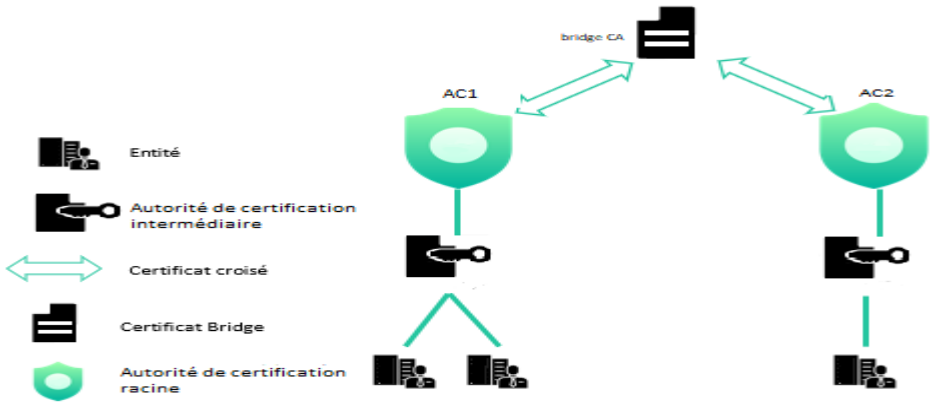

Figure 9 Architecture en pont

2.8.2.4. Architecture hybride

La PKI hybride peut connecter une PKI d'architecture hiérarchique et une PKI Peer to peer. Dans ce cas, la certification croisée est utilisée pour connecter les différentes PKI en une seule PKI hybride [11]. Cela permet aux parties dépendantes l'une à l'autre de vérifier et d'accepter les certificats produits par l'autre PKI. (Voir Fig.10) :

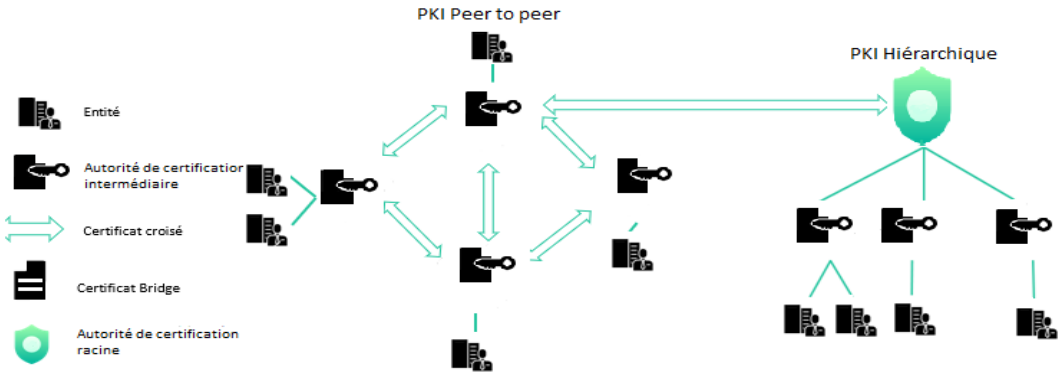

Figure 10 Architecture Hybride

2.8.2.5. Comparaison entre les architectures

Dans cette partie, nous allons approfondir notre analyse en mettant en évidence une comparaison entre les différentes architectures de PKI que nous avons préalablement mentionnées. Nous examinerons en détail leurs avantages et leurs limites, afin d'apporter une vision claire et comparative des options disponibles. (Voir Tab.1)

Architecture	Avantages	Inconvénients
Hiérarchique	• La conception et la validation du chemin de certificat sont simples. • Évolutif et scalable.	• Une fois que la clé privée de Root AC fuit, le modèle est en panne.
Peer to Peer	• Les certificats ont plus d'extensions. • Intégrer facilement une nouvelle communauté d'utilisateurs.	• Le processus de validation de chemin est plus complexe [11]. • Le coût de gestion est élevé.
Pont	• Interopérabilité entre les PKI.	• La confiance sera complètement détruite s'il y a une attaque sur le certificat bridge.
Hybride	• Interconnexion de différentes architectures PKI.	• La vérification du chemin du certificat est complexe.

Tableau 1 Comparaison entre les Architectures PKI

2.8.2.6. Conclusion

En conclusion, l'analyse comparative des architectures de PKI que nous avons examinées met en évidence une diversité d'options et de considérations. Chaque architecture présente des avantages et des limites spécifiques, et le choix final dépendra des besoins et des objectifs particuliers de chaque organisation. Il est crucial de prendre en compte des aspects tels que la sécurité, la scalabilité et la facilité de déploiement lors de la sélection de la PKI appropriée. En comprenant les forces et les faiblesses de chaque architecture, il est possible de faire des choix éclairés qui garantiront la mise en place d'un système de PKI robuste et efficace pour répondre aux besoins spécifiques de l'organisation.

2.8.3. Avantages du PKI

L'utilisation d'une PKI offre de nombreux avantages :

- L'utilisation d'une PKI devient légèrement plus sécuritaire que les mots de passe, car afin d'usurper l'identité d'un utilisateur valide, les utilisateurs malveillants ou les attaquants doivent démasquer à la fois la phrase secrète correspondante et la clé privée.
- La PKI fournit une vérification d'identité renforcée grâce à des clés privées et secrètes.
- Puisque la PKI peut accueillir un nombre illimité d'utilisateurs, elle consiste en une infrastructure très évolutive. [12]
- Seul le propriétaire désigné de la clé peut décoder les données lors de l'utilisation d'opérations de chiffrement unidirectionnel.
- La PKI utilise des clés privées difficiles à casser avec la clé publique correspondante.
- Les PKI permettent des offres de services sécuritaires pour les banques, le droit, les soins de santé, le commerce électronique et le renseignement, et ce, grâce à l'utilisation de signatures numériques et de certificats numériques.
- Elle détecte la falsification et permet la non-répudiation. [12]

2.8.4. Inconvénients de la PKI [12]

Comme mentionné précédemment, l'utilisation de la PKI offre certains avantages, cependant, Elle a aussi des inconvénients comme :

- La principale faiblesse de PKI s'établit par le fait qu'un certificat peut être signé par n'importe quelle AC pour un individu ou une machine. Il y a aussi la situation où les AC sont obligés de livrer des certificats pour des entités dont elles n'ont pas à se porter garantes.
- Le modèle de certification donne le pouvoir d'approbation des certificats X.509 entre les mains de certains spécialistes agissant de manière incompétente ou malintentionnée. Lorsqu'une autorité de certification provient d'une action malintentionnée, elle peut émettre des certificats

malveillants ne respectant pas les normes et les meilleures pratiques. Les PKI dépendent fortement de l'intégrité des AC et des AR et ceux-ci ne sont pas toujours parfaitement fonctionnels d'un point de vue professionnel de conscience et de contrôle.

- L'échec d'une clé de signature d'une AC représente une catastrophe. Les clés pourraient être compromises à l'insu de quiconque. Puisque la gestion et la révocation des certificats nécessitent une structure très compliquée, cette complexité devient une faiblesse de la visibilité pour la PKI.

2.8.5. PKI avec le standard ISO15118

Comme indiqué dans la norme ISO 15118, l'infrastructure à clé publique hiérarchique X.509 est recommandée [5]. Elle sous-tend les protocoles de sécurité conçus pour faire face aux principales menaces affectant l'interface entre les utilisateurs du VE et la borne de recharge. Elles se concentrent sur :

- *Sécurité des données :* la confidentialité se veut essentielle pour la confiance des utilisateurs afin que les fournisseurs de services adhèrent aux réglementations de sécurité des données. Aussi, ceci permet d'empêcher l'extraction d'informations telles que les clés de session qui pourraient être utilisées dans des attaques. Selon la norme ISO 15118, les données envoyées et reçues doivent subir un chiffrement et un déchiffrement à l'aide d'une infrastructure à clé publique.

- *Authentification sécurisée :* dans le cadre de la PKI, les certificats numériques sécurisés garantissent que les parties impliquées sont bien celles prétendues avant tout échange de données. Ceci importe pour les services publics afin d'assurer que tous les utilisateurs de l'infrastructure énergétique demeurent valides.

- *Intégrité des données :* les protocoles de sécurité doivent garantir que tous les messages et données envoyés entre les acteurs communicants demeurent inaltérés pendant le transit.

Les mécanismes essentiels pour la sécurité dans une session de communication s'obtiennent grâce à une combinaison d'algorithmes cryptographiques symétriques et asymétriques utilisant une PKI. Le processus de la sécurité selon la norme ISO 15118, ce processus, en termes simplifiés, ressemble à :

- *Étape 1 :* TLS handshake authentifie les deux parties à la session.
- *Étape 2 :* À l'aide d'un protocole Elliptic Curve Diffie-Hellman (ECDH), une clé de session commune est convenue et partagée.
- *Étape 3 :* Les données et les messages échangés utilisent AES-128 pour le cryptage.
- *Étape 4 :* L'authentification de l'utilisateur et l'intégrité des messages sont vérifiées à l'aide de l'algorithme Elliptic Curve Digital Signature Algorithm (ECDSA).

Les Autorités de certification jouent un rôle important dans le fonctionnement de la PKI. La confiance dans ces certificats permet une authentification sécurisée des parties communiquant selon le protocole. Il existe également les AC subordonnées qui livrent les certificats aux entités finales. Dans ce qui suit, les différents types de certificats proposés dans la norme ISO 15118 seront présentés. (Voir fig.11) :

- *Certificat Racine V2G*

Il s'agit de certificats racines valides (niveau supérieur) de la PKI. Ils sont utilisés pour vérifier l'authenticité des certificats. Les clés privées correspondantes sont en possession des autorités de certification racine respectives.

- *Certificat racine d'opérateur de mobilité*

Ce certificat est utilisé pour signer (par une chaine des AC subordonnées) des certificats de contrat.

- *Certificats de contrat*

Ce type de certificat est utilisé dans le cas d'utilisation Plug and Charge (PnC) pour représenter un contrat entre un véhicule et un acteur secondaire (l'opérateur de mobilité). Il est stocké dans un EVCC avec la clé privée correspondante. L'EVCC l'utilise pour prouver l'existence du contrat correspondant à l'EVSE. Les certificats de contrat sont dérivés d'un certificat racine d'opérateur de mobilité.

- *Certificat SECC*

Ce certificat est utilisé pour authentifier le SECC auprès de l'EVCC. La clé privée correspondante est en possession du SECC. Les certificats SECC sont dérivés des certificats racine V2G mentionnés ci-dessus.

- *Certificat racine d'opérateur privé*

Le certificat racine d'opérateur privé acquiert des similarités avec le certificat racine d'opérateur de mobilité. La seule différence se trouve dans la gestion du plan organisationnel. Son objectif sert à faciliter la mise en place d'infrastructures de recharge privées pour les voitures sous le contrôle immédiat du propriétaire de l'infrastructure.

- *Certificat d'approvisionnement original Equipment Manufacturer (OEM)*

Ce type de certificat est individuel pour chaque véhicule (installé par exemple lors de la production du véhicule) et utilisé pour vérifier l'identité d'un véhicule au début du processus d'approvisionnement.

- *Certificat racine OEM*

Ce certificat est utilisé pour signer les certificats d'approvisionnement OEM. Chaque OEM peut créer un certificat racine (de niveau supérieur) et le distribuer aux acteurs secondaires. Le certificat racine d'un OEM ne fait pas partie de la PKI globale, c'est-à-dire qu'il n'est pas nécessairement signé par un certificat racine V2G.

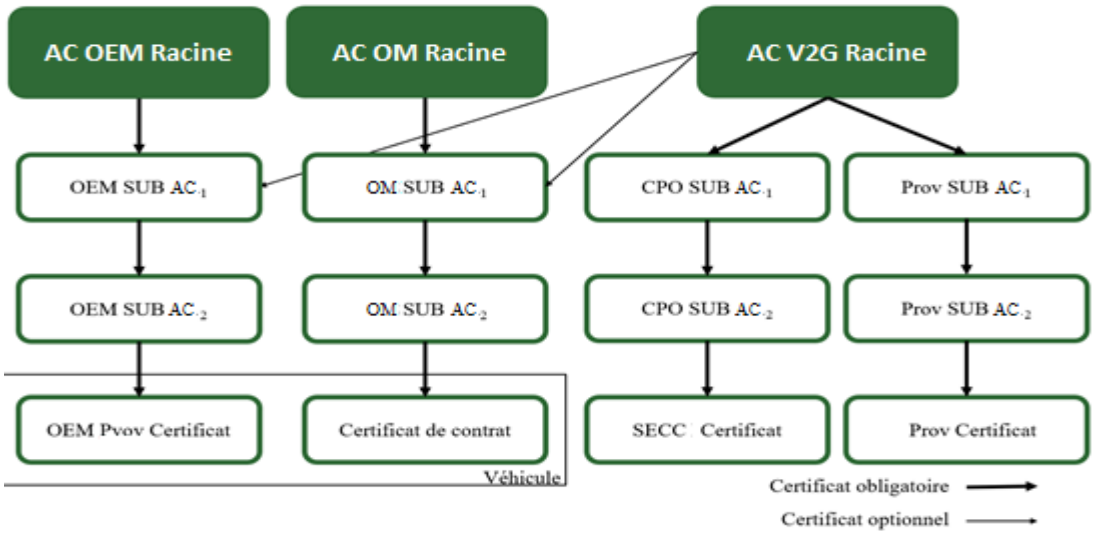

Figure 11 Certificats selon la norme ISO15118

La communication entre le VE et la borne se place au cœur du réseau V2G. Il est primordial de sécuriser les différents messages afin de les défendre contre des attaques éventuelles, car ils peuvent contenir des données de natures diverses dont certaines sont privées. Nous avons fourni un aperçu de l'architecture de sécurité du réseau V2G ainsi que les exigences de sécurité et les difficultés rencontrées par les réseaux V2G. Dans le chapitre suivant, nous allons revenir sur la littérature des PKI dans les réseaux V2G, la sécurité des chaines de blocs ainsi que les PKI inter domaine en discutant les points forts et faibles de chaque modèle proposé.

Chapitre III

État de l'art

Depuis que de nombreuses statistiques ont commencé à montrer la croissance des infrastructures V2G, plusieurs recherches et protocoles qui couvrent la sécurité sur les réseaux V2G ont été proposés, plus particulièrement l'utilisation des PKI. Dans ce chapitre, nous présenterons un aperçu de la littérature sur l'infrastructure à clés publique (PKI) dans les réseaux V2G, les mécanismes de sécurité des chaines de blocs et ainsi les PKI multi domaines pour les réseaux V2G.

3.1. Les réseaux V2G

Plutôt en 2019, Gope et Sikdar [13] ont proposé un mécanisme d'authentification simple pour les interactions V2G qui protège la confidentialité. Ce mécanisme utilise des primitives cryptographiques légères telles que des fonctions de hachage unidirectionnelles et des opérations de ou exclusives (XOR). Leur système suggéré offre une confidentialité de localisation avec un cout de calcul très léger et une résistance aux cyberattaques bien connues, en particulier du côté des VE. Malheureusement, il n'y a aucune sécurité physique.

Dans un effort pour augmenter l'efficacité des méthodes d'authentification basées sur des courbes elliptiques non super singulières (NSSEC), Su et al. [14] ont introduit un nouveau mécanisme d'authentification préservant la confidentialité pour les communications V2G basé sur les NSSEC. Néanmoins, leur technique suggérée nécessite des primitives cryptographiques lourdes en plus d'avoir l'inconvénient du schéma de Gope dans [13].

Un protocole d'accord clé (key agreement) pour les réseaux V2G basé sur une carte chaotique Chebyshev sans séquestre a été présenté par Abbasinezhad Mood et

al. [15]. Bien qu'ils offrent de bonnes fonctionnalités de sécurité, leur plan souffre toujours d'un manque de confidentialité de localisation, de sécurité physique et d'une conception volumineuse.

Han, M., et al. ont suggéré un système d'authentification anonyme basé sur l'informatique du brouillard (fog computing) dans [16]. Ce dernier est fait pour répondre aux problèmes de congestion du réseau qui surviennent lors des communications entre l'AC et les voitures lors de l'échange de pseudonymes. L'informatique du brouillard est utilisée pour configurer et suivre les pseudonymes, ce qui permet d'assurer une communication en temps réel et de réduire le besoin de réauthentification. Ce protocole répond également aux exigences de sécurité des réseaux informatiques, malgré son taux de perte de paquets assez élevé.

Bansal et al. [17] ont présenté une stratégie d'authentification mutuelle pour V2G utilisant des fonctions physiques non clonables (PUF). Selon [18], la seule conception qui pourrait résister à une agression physique est celle proposée dans [17]. Pourtant, leur schéma ne garantit pas la confidentialité des véhicules contre la société vendeuse. De plus, leur plan est mal conçu en termes de cout de calcul du côté des VE.

Les auteurs de [25] ont proposé un système de protection de confidentialité basé sur le protocole Diffie-Hellman pour créer dynamiquement des clés de session, puis effectuer une authentification sécurisée afin de protéger les informations de facturation dans le réseau V2G. Ils ont retiré l'AC du processus de communication entre les entités du réseau V2G pour optimiser le calcul du temps. De même, ils ont utilisé une approche de transmission de données anonyme pour garantir l'anonymat. Sans avoir besoin d'un tiers fiable, ce protocole protège l'anonymat et le secret des données dans le réseau V2G. Cependant, il ne protège pas l'intégrité des données et son efficacité n'a pas été testée par des simulations.

3.2. Les chaines de blocs dans les réseaux V2G

En mettant l'accent sur les algorithmes de consensus distribués, la taxonomie de l'architecture de la chaîne de blocs, ainsi que la pertinence de certains algorithmes dans les réseaux intelligents. Andoni, M. *et al* [19] ont présenté les composants fondamentaux nécessaires de technologie de registres distribués (DLT) au commerce de l'énergie. Les difficultés qui pourraient survenir lors de la création d'une plateforme d'échange d'énergie pour le réseau V2G ont également été explorées.

Les auteurs de [20] ont introduit un mécanisme d'authentification hiérarchique assisté par une blockchain et la cryptographie à courbes elliptiques (ECC) pour l'environnement V2G. Pour l'authentification hiérarchique dans leur étude, ils ont utilisé la cryptographie à courbe elliptique (ECC). Ce mécanisme est utilisé pour assurer l'anonymat des VE. En même temps, d'offrir une authentification mutuelle entre les VE et les bornes de recharge. Ils ont divisé le modèle de système en quatre étapes : 1-initialisation du système, 2-enregistrement (Registration), 3-authentification mutuelle hiérarchique et 4-consensus. Dans les environnements V2G distribués, la technologie des registres distribués d'une blockchain (blockchain's distributed ledger) a été utilisée pour exécuter des transactions. La défense contre diverses menaces a été vérifiée à l'aide de l'outil Automated Validation of Internet Security Protocols and Apps (AVISPA). Cependant, le modèle de menace n'est pas correctement discuté et le mécanisme proposé n'a pas été évalué pratiquement.

Un réseau V2G basé sur la blockchain pour le partage de données et le commerce d'énergie a été proposé par Hassija et al. [21]. Il vise à relever les défis du partage de données dans les environnements véhiculaires en exploitant la technologie de la blockchain. L'objectif principal du modèle est de permettre un partage léger des données tout en garantissant la sécurité, la confidentialité et l'efficacité. Il y parvient en utilisant les propriétés intrinsèques de la blockchain telles que le consensus décentralisé, l'immutabilité et la transparence. Pour les transactions énergétiques entre la borne de recharge et les VE au moindre coût possibles, les auteurs ont utilisé la théorie des jeux.

De la même manière, les auteurs de [22] ont suggéré une stratégie d'échange d'énergie pour les VE basée sur la blockchain afin de réduire les fluctuations de puissance. Leur modèle utilise la blockchain pour enregistrer et vérifier les transactions liées à la participation des VE, notamment la fourniture d'énergie, la demande de charge et la gestion de l'énergie. Cela permet de garantir la transparence, l'intégrité et la sécurité des données, ainsi que d'assurer la confiance entre les différents acteurs du système. En utilisant ce schéma, l'intégration des VE devient plus fluide en termes de réduction des fluctuations de puissance et des coûts de recharge. Toutefois, La plateforme distribuée dans la blockchain fait face à des obstacles sérieux tels que le manque de robustesse, une structure réseau sécurisée et un mécanisme d'authentification [23].

Les auteurs dans [24] introduisent un mécanisme décentralisé d'authentification et d'échange de clés pour les scénarios de calcul en brouillard pour VE. Ce mécanisme est basé sur la blockchain et la cryptographie à courbes elliptiques. La blockchain est utilisée pour maintenir les informations des réseaux, tandis que l'ECC est adopté pour assurer une authentification mutuelle entre les véhicules et les nœuds de brouillard. Ce modèle est meilleur que les autres modèles non basés sur la blockchain en termes d'anonymité des utilisateurs, l'authentification mutuelle, la confidentialité de l'identité de l'utilisateur et la confidentialité des données. Cependant, leur travail ne discute pas les détails de l'analyse de sécurité, c'est-à-dire le modèle de menace, les hypothèses, etc.

3.3. PKI multi Domain pour les réseaux V2G

Dans [25] Binod et al. ont suggéré un modèle PKI multi-domaine pour le réseau V2G qui est construit sur la cryptographie à courbe elliptique et une publique auto certifiée technique de clé ayant un certificat implicite. La proposition du protocole n'a été comparée qu'au modèle PKI proposé dans ISO 15118 et non à d'autres protocoles. Ils annoncent un temps de traitement des certificats dans leur système plus rapide que le système proposé dans la norme standard. Ce protocole ne

protège pas l'anonymat à toutes les étapes de la communication. De plus, l'efficacité de leur modèle n'a pas été établie par une modélisation formelle ni une simulation.

Dans [26] Mohamed et al. ont proposé une PKI hiérarchique entièrement connectée qui prend en compte des caractéristiques de smart grid. Dans la clé publique proposée, chaque AC est responsable de gérer les certificats de clé publique pour une petite zone géographiquement délimitée. Ils ont également suggéré un nouveau format pour les certificats qui lie non seulement l'identité d'un nœud à sa clé publique, mais aussi à ses privilèges et autorisations. Enfin, ils ont proposé un système de renouvellement de certificat efficace et évolutif qui peut réduire considérablement les frais généraux liés au renouvellement des certificats. Leur modèle proposé a été évalué sur un seul domaine PKI. De même, il a été évalué sur un PKI multi-domaines pour Smart Grid. Leur application de multi-domaine n'assure aucun anonymat des entités puisque l'identité est liée à la clé publique et la validité du protocole proposé n'a été examinée par aucune modélisation ou simulation officielle.

L'anonymat était bien préservé dans [27] lorsque les auteurs ont proposé un schéma d'authentification en fonction de l'état de la batterie (BASA). Le BASA à un identifiant agrégé pendant la charge complète (CC), la transition d'état était pour garantir que les véhicules peuvent être authentifiés sans divulguer leurs identités réelles. Également, il effectue une réponse sélective basée sur la divulgation d'authentification pendant la CC à la phase de décharge pour réaliser l'échange de données anonyme. Ils ont préservé la confidentialité des données et aussi l'intégrité, mais les preuves agrégées causent d'énormes surcharges dans le processus de communication.

Fondamentalement, les énormes surcharges dans le processus de communication sont parvenues à une solution en 2021 quand Xia et al. [28] ont proposé un cadre basé sur une identité de tarification d'authentification formée sur l'informatique en brouillard qui réduit considérablement le nombre d'interactions

avec les serveurs cloud distants et en plus, minimiser leur charge de calcul. La solution proposée améliore aussi l'efficacité de la communication entre les entités du réseau V2G. Le schéma proposé peut être repris en 4 étapes :

1- Toutes les entités notamment : Le VE, les serveurs d'électricité (ES), le serveur de brouillard (FS) envoient leurs identifiants à l'AC, par la suite, l'AC génère une clé publique/privée.
2- Après réception de la demande de recharge, le FS authentifie l'utilisateur du VE et il interagit avec le VE juste initialement pas fréquemment.
3- L'utilisateur de FS et le VE confirment l'exactitude des informations de facturation ou plutôt les informations de chargement (IC).
4- Le serveur d'électricité audite l'information de chargement du FS régulièrement, ce qui garantit la cohérence des données.

Ce protocole est prouvé par le formulaire modèle formel POR. Cependant, la non-répudiation n'est pas assurée et cela ne protège pas la vie privée du réseau et du VE lui-même.

Dans [29] Binod et al. ont proposé une architecture de réseau multi-domaine pour les réseaux V2G qui comprend une solution hybride complète à clé publique utilisant la hiérarchie et la certification croisées peer-to-peer. L'architecture de sécurité proposée est basée sur la cryptographie à courbe elliptique et la certification implicite contrairement à la certification explicite traditionnelle. Ils ont mentionné que le chemin de validation du certificat dans leur modèle est moins que le modèle standard. Mais, loin d'être trop complexe à déployer. Ce modèle n'a été formulé par aucune modélisation formelle ni par une simulation.

En général, Les protocoles pour les réseaux V2G proposés dans la littérature ne répondent pas à certaines exigences importantes en matière de sécurité informatique, tels que l'anonymat et la non-répudiation. L'analyse de ces protocoles nous a permis d'identifier leurs avantages, d'étudier leurs lacunes que nous avons identifiées et d'être en mesure de proposer un schéma robuste qui prend en charge une relation de confiance PKI inter domaine qui dépasse également les exigences de base de la norme ISO 15118 qui ne prend pas en charge la PKI inter domaine pour les

réseaux V2G. Notre protocole sera basé sur l'anonymat et comprendra une authentification mutuelle obligatoire entre le VE et la grille et tous les certificats racine. Dans notre schéma, nous utiliserons des certifications croisées entre les AC racine, cela permettra aux domaines PKI de construire efficacement des relations de confiance. Les AC racine de divers domaines peuvent se certifier mutuellement à l'aide des certifications croisées afin que toutes les entités puissent créer des connexions fiables avec l'entité finale dans d'autres domaines.

Chapitre IV

Description du modèle de sécurité

Dans notre modèle, le système V2G est entièrement autonome et regroupe plusieurs domaines V2G. Chaque domaine, se compose d'une AC de confiance (Root AC) et d'un nombre d'entités à l'intérieur du domaine (soit les AC subordonnées, les VE et les bornes de recharge). Un modèle PKI hybride a été mis en œuvre avec une confiance de certification croisée peer-to-peer pour les AC racine. Un modèle de confiance hiérarchique pour les AC subordonnés est mis en place.

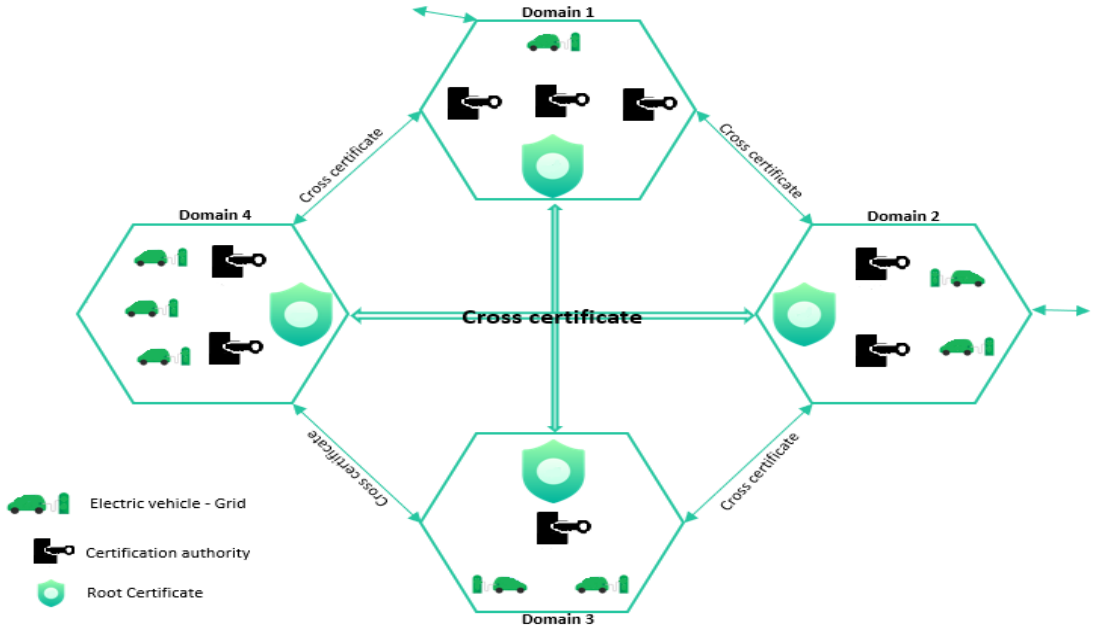

Figure 12 Schéma du modèle proposé

L'utilisation du cross certification peer-to-peer est de pallier les lacunes du standard PKI pour les réseaux V2G existants, puisqu'il ne prend pas en charge la communication inter domaine. En utilisant cette approche, nous pouvons également éviter les conflits de politique entre les domaines. Ainsi, les entités dans un domaine spécifique pourront communiquer avec n'importe quelle autre entité dans un autre domaine sans conflits de politique entre eux. Ce qui était la principale raison de l'échec de la communication PKI inter domaine. (Voir Fig.12)

L'objectif de ce modèle PKI est faciliter et sécuriser les échanges d'informations entre différents domaines. Les deux approches cryptographiques ont été utilisées, asymétrique pour l'échange des clés et symétrique pour l'échange des messages sécurisés principaux lors de la session de communication.

4.1. Primitives et symboles

4.1.1. Certificat croisé

C'est un certificat émis par une AC qui signe la clé publique d'un autre AC ne faisant pas partie de sa hiérarchie de confiance. [30] Le certificat croisé établit une relation de confiance entre les deux AC. Il est plus sécurisé et permet d'avoir les traces de toutes les transactions effectuées.

4.1.2. Table de Symboles

Symbole	Signification
IDev	ID de VE
IDg	ID de la borne de recharge
RKev	Clé Aléatoire de EV
RKg	Clé Aléatoire de la borne de recharge
PBev,PRev	Clé Publique/Privée de VE
PBg,PRg	Clé Publique/Privée de la borne de recharge
vRCAx	Clé de Vérification de Root AC numéro x
PCGev	Génération du pseudo-entité pour le VE
PVGev	Vérification du pseudo-entité pour le VE
PCGg	Génération du pseudo-entité pour la borne
PCVg	Vérification du pseudo-entité pour la borne
PBRCAx,PRRCAx	Clé Publique/Privée pour la Root AC numéro x

Tableau 2 Symboles utilisés dans le protocole proposé

4.2. Détails du protocole proposé

4.2.1. Première phase : Certification croisée peer-to-peer entre les AC racines

Par définition [30], l'idée est la mise en place d'une relation de confiance entre deux AC, par exemple RCAx et RCAy. Pour que cela se produise, deux RCA doivent solidement échanger leurs clés de vérification. Autrement dit, le RCAx chiffre sa clé

de vérification (vRCAx) avec la clé publique de RCAy et l'envoie à RCAy. Ce dernier déchiffre le message reçu avec sa clé privée. Le même scénario se produit du côté de RCAy. Ces clés sont utilisées pour vérifier les signatures sur les certificats. Lorsque chaque RCA vérifie l'identité de l'autre, RCAx crée et signe un certificat contenant la clé publique de RCAy et vice versa, par la suite RCAx et RCAy le diffusent chacune à son domaine respectif. (Voir Tab.2 pour faire référence au symbole).

4.2.2. Deuxième phase : Authentification du véhicule électrique

Dans un scénario où un VE du domaine 2 souhaite établir une communication sécurisée avec la borne dans le domaine 4 (voir figure 13), l'ancrage de confiance du VE est RCA2 et l'ancrage de confiance de la borne de recharge est RCA4, la borne doit établir une chaîne de confiance depuis son ancrage de confiance jusqu'au certificat du VE. Au moment où la borne reçoit le certificat du VE, elle tente de vérifier la signature. Pour se faire, l'ancrage de confiance de la borne, la RCA4, a signé la clé publique de RCA2 établissant une co-certification (établie au point précédent). Ensuite, RCA2 a signé la clé de vérification du VE donc la vérification est complétée. Dans une explication plus détaillée, nous décrirons la cinématique des messages de communication échangés durant l'entièreté de la procédure d'authentification du VE.

Le VE génère une clé aléatoire (RKev) utilisée à des fins de chiffrement symétrique puis il envoie la clé combinée avec son identité (IDev) au RCA2. Ce message est crypté par la clé publique du RCA2 (PBRCA2) pour assurer que seulement RCA2 obtiendra cette combinaison. La RCA2 déchiffre le message avec sa clé privée (PRRCA5) puis elle génère une seconde clé privée et publique (PRev, PBev) du VE et deux clés aléatoires qui sont :

- *Première clé aléatoire : pour* générer sa pseudo-entité et son certificat (PCGev).
- *Deuxième clé aléatoire : pour* valider sa pseudo-entité et son certificat (PCVev)

Comme étape finale, le RCA2 crypte le message {PCGev, (PRev, PBev)} avec (RKev) et l'envoie au VE. Ensuite, il signe (PCVev) en utilisant sa clé privée. Pour continuer le processus, RCA2 crypte cette signature avec la clé publique du RCA4 pour le lui envoyer. Comme les deux autorités possèdent déjà une certification croisée, RCA4 déchiffre le message avec sa clé privée et vérifie la signature avec (PBRCA2). Par la suite, elle récupérera la (PCVev) qui est la clé de la vérification du pseudo entité et du certificat du VE pour l'envoyer aux bornes qui sont dans son domaine. La borne dispose maintenant de (PCVev) et peut vérifier le certificat et l'identité du VE qui souhaite établir une communication sécurisée. (Voir Fig.13)

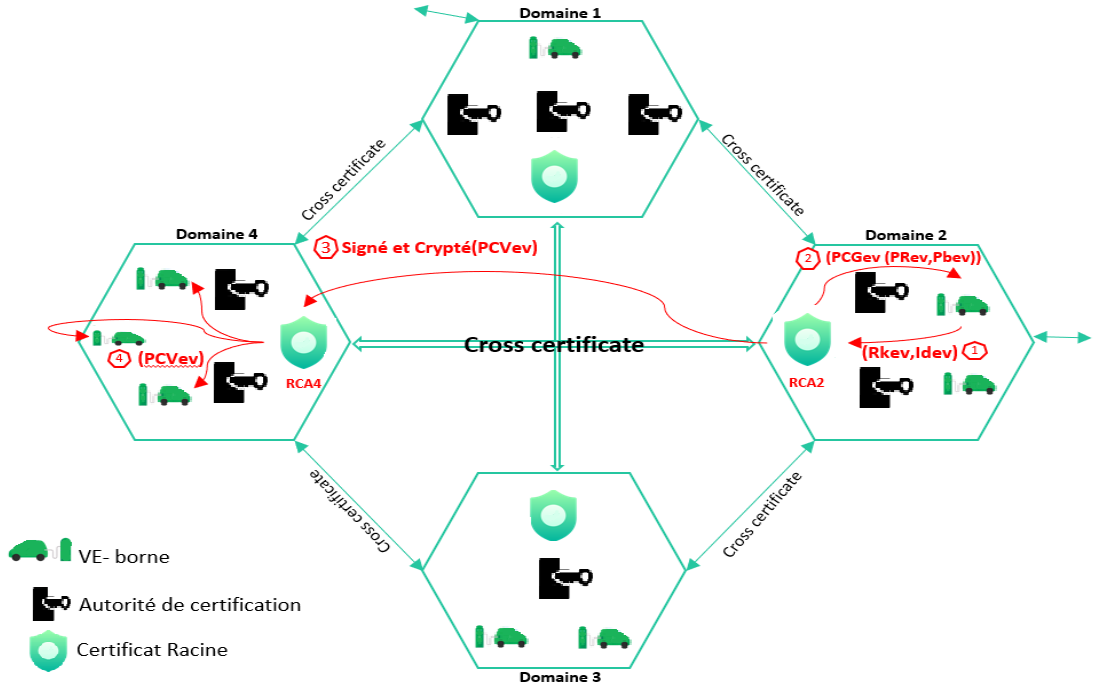

Figure 13 Étapes d'authentification du VE

4.2.3. Phase 3 Authentification de la borne

L'authentification de la borne suit les mêmes étapes que l'authentification du VE. Dans ce scénario, l'ancrage de confiance de la borne est RCA4, la borne génère une clé aléatoire (RKg) afin de l'utiliser pour le chiffrement symétrique puis elle envoie la clé avec son identité (IDg) au RCA4. Ce message sera crypté par la clé publique de RCA4 (PBRCA4) afin d'assurer que seul RCA4 obtient cette clé et l'ID de la borne. La RCA4 déchiffre le message avec sa clé privée (PRRCA4) puis, elle

génère la clé privée et publique (PRg, PBg) de la borne et deux clés aléatoires qui sont :

- *Première clé aléatoire :* clé pour générer sa pseudo-entité et son certificat (PCGg).
- *Deuxième clé aléatoire :* clé pour valider sa pseudo-entité et son certificat (PCVg).

Comme étape finale, RCA4 crypte le message {PCGg, (PRg, PBg)} avec (RKg) et l'envoie à la borne. Ensuite, elle signe (PCVg) en utilisant sa clé privée et le crypte avec la clé publique de RCA2 pour la lui envoyer. Comme on a déjà mentionné qu'ils ont déjà une certification croisée établie, RCA2 déchiffre le message avec sa clé privée et vérifie la signature avec la clé publique de RCA4 (PBRCA4) puis récupère la (PCVg) qui est la clé de la vérification du pseudo entité et le certificat de la borne et l'envoie aux VEs qui sont dans son domaine. Le VE a maintenant (PCVg) et peut vérifier le certificat et l'identité de la borne avec qui il souhaite établir une communication sécurisée.

4.2.4. Établissement de la communication

Au moment où le VE reçoit le message de RCA2, il le déchiffre et vérifie la signature du RCA2, puis il génère son pseudo entité et son certificat à l'aide de PCGev et l'envoie à la borne. Ensuite, la borne déchiffre le message par sa clé publique et tente de vérifier l'identité du VE à l'aide de PCVev qu'elle a obtenu de RCA4. Si la vérification a réussi, la borne envoie sa pseudo-entité et son certificat au VE crypté par PBev et ce dernier peut authentifier la borne avec le (PCVg) qu'il a obtenu de RCA2. Comme dernière étape, le véhicule négocie une clé de session basée sur RKev et RKg, puis démarre la communication en utilisant le protocole Transport layer security (TLS) en toute sécurité. Un résumé détaillé du protocole l'échange de messages est résumé dans la figure 14 ci-dessous.

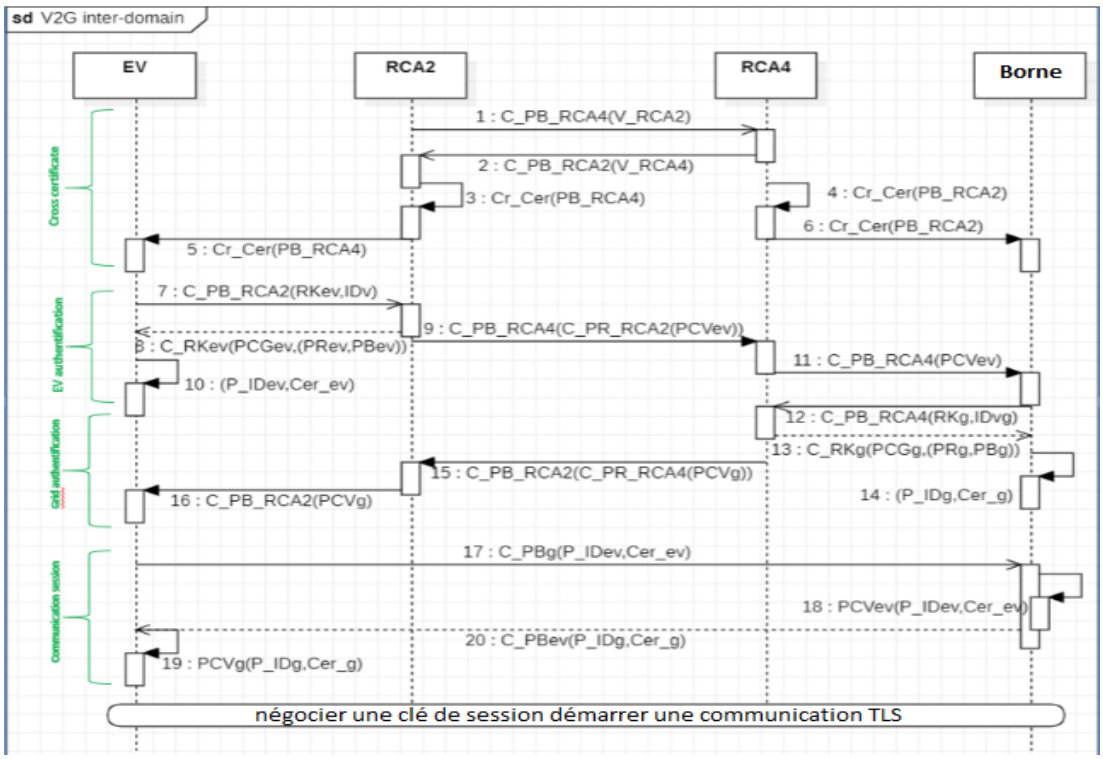

Figure 14 Échanges des messages durant toute la procédure de communication inter Domain

4.3. Analyse théorique de la sécurité

Dans ce chapitre, nous avons présenté un modèle de sécurité pour le système V2G multi domaine. Pour assurer sa robustesse et sa fiabilité, une analyse théorique de la sécurité a été réalisée, prenant en compte les points suivants :

Confidentialité : Le modèle garantit la confidentialité des échanges en utilisant des méthodes de cryptographie, notamment l'échange de clés asymétriques et symétriques. Les informations sensibles sont protégées contre les accès non autorisés.

Intégrité : L'utilisation de certificats et de signatures numériques assure l'intégrité des données échangées. Toute modification non autorisée des informations est détectée, ce qui permet de prévenir les attaques de falsification.

Authentification : Le modèle propose un processus d'authentification robuste pour les VE et les bornes de recharge. Les certificats et les clés de vérification permettent de vérifier l'identité des entités et d'établir une confiance mutuelle.

Non-répudiation : Grâce à l'authentification mutuelle et à l'utilisation de signatures numériques, le modèle garantit la non-répudiation des transactions. Ainsi, aucune des parties ne peut nier son implication dans un échange.

Anonymat : L'utilisation de pseudo-entités permet de préserver l'anonymat des entités impliquées dans les échanges. Cela renforce la confidentialité des données personnelles des entités.

Résistance aux attaques : Le modèle a été conçu pour résister à diverses attaques courantes, telles que l'usurpation d'identité, l'interception de données et la falsification de certificats. Les mécanismes de sécurité mis en place réduisent les vulnérabilités potentielles.

Au prochain chapitre, une analyse plus détaillée du protocole sera effectuée. Cela inclura des simulations, des tests et une évaluation approfondie de la solidité et de la fiabilité du modèle de sécurité proposé.

Le modèle de sécurité présenté dans ce chapitre offre une approche solide pour sécuriser les échanges d'informations dans le système V2G. Il prend en compte les principaux aspects de la sécurité, tels que la confidentialité, l'intégrité, l'authentification et la non-répudiation, tout en préservant l'anonymat des entités impliquées. Cependant, une évaluation plus approfondie de sa résistance aux attaques sera réalisée dans le chapitre suivant pour confirmer sa robustesse.

4.4. Conclusion

La confidentialité a été assurée en utilisant la cryptographie. L’utilisation des certificats et des signatures numériques a rendu le protocole sécuritaire. L’authentification mutuelle combinée à l’intégrité assurent la non-répudiation, l'utilisation des pseudo-entités nous garantit l'anonymat. La vérification et la solidité du protocole sera présentée au chapitre suivant. Nous allons dans un premier temps présenter les différentes simulations que nous avons effectuées, l'environnement dans lequel ces simulations ont été réalisées et enfin la méthodologie suivie.

Chapitre V

Modélisation et simulation

Dans ce chapitre, les différentes simulations présentées aux termes de notre recherche ont été réalisées sur un seul ordinateur physique, simulant de manière logicielle la présence des différentes entités du réseau (VE et la borne). Nous allons résumer les principaux outils que nous avons utilisés lors de la modélisation et de la simulation de notre protocole.

La modélisation a été réalisée avec l'outil Tamarin Prover, tandis que la simulation des sessions de communication avant chargement a été réalisée avec RISE V2G. Comme dernier test, la simulation des attaques a été faite avec Kali Linux. Ce sont des outils que nous avons choisi, car leurs caractéristiques sont bien adaptées aux réseaux V2G. L'ordinateur utilisé possède les caractéristiques décrites dans le tableau ci-dessous. (Voir Tab.3)

Machine	Dell
Système d'exploitation	Ubuntu 20.04 LTS
Nombre de cœur physique	6
Nombre de cœur logique	12
Mémoire Vive	32 Gb
Processeur	Inter core i9 – 2.90 GHz

Tableau 3 caractéristiques de machine

5.1. Outils de modélisation

5.1.1. Tamarin Prover

Tamarin Prover est un logiciel de vérification formelle des protocoles cryptographiques. C'est un outil puissant pour la modélisation symbolique et l'analyse des protocoles de sécurité [31]. De plus, Tamarin Prover est un outil de

vérification de protocole de sécurité qui permet à la fois la falsification et la vérification illimitée dans le modèle symbolique. Il a été utilisé pour vérifier la communication avec le protocole Transport Layer Security 1.3 [32] et aussi ISO/IEC 9798 [33].

5.1.2. Méthodologie

Comme Tamarin Prover est un outil pour la modélisation et l'analyse de protocoles de sécurité [34], il nous permettra de confirmer le fonctionnement et l'efficacité de notre protocole contre les attaques de l'homme du milieu. Tamarin offre une large gamme de fonctionnalités intégrées telles que Diffie Hellman, hachage, cryptage symétrique et asymétrique. En utilisant Tamarin Prover, nous pouvons construire et spécifier un modèle d'adversaire pour vérifier les propriétés de sécurité du protocole.

Le réseau sera contrôlé par un modèle d'adversaire et par conséquence Tamarin peut injecter, modifier et supprimer les paquets échangés dans le réseau.

Afin de vérifier les propriétés de sécurité, nous avons utilisé essentiellement des règles de génération de clé aléatoire, des règles de signature, des règles asymétriques de génération et de diffusion de clés. Nous avons également défini plusieurs lemmes dans le but de vérifier la stabilité du protocole et d'identifier les attaques attendues. (Voir Fig.15).

```
////////////////////////////////<>////////////////////////////////////////////////LEMMAS/////////////////////////////////

////////////SEND_RECV BETWEEN RCAs
lemma There_Is_At_SomePoint_a_Cross_certificate:
exists-trace
"Ex RCAX RCAY VRK #i #j.
Send(RCAX, VRK) @i
& Recv(RCAY, VRK) @j "


lemma it_cannot_be_that_an_rcax_has_generated_a_VRK_and_the_attacker_knows_it:
all-traces
"All VRK #i. Secret(VRK) @i & Role('RCAX') @i ==> (not (Ex #j. K(VRK)@j)) | (Ex RCAY #j. Reveal(RCAY)@j & Honest(RCAY)@i)"

//////////AUTHENTIFICATION
lemma Authentic_CC:
"All b m #i.
Authentic(b, m) @i
==> (Ex #j. Send(b, m) @j & j<i)"


////////////////////////SIGNING OF CROSS CERTIFICATES
restriction Equality:
"All x y #i. Eq(x,y) @i ==> x = y"
lemma communicate_RCAs:
exists-trace
"Ex RCAX RCAY m #i #j. Send(RCAX,m)@i & Recv(RCAY,m) @j"
lemma message_authentication_RCAs:
"All b m #i. Authentic(b,m) @i
==> (Ex #j. Send(b,m) @j & j<i)
| (Ex RCAY #r. Reveal(RCAY)@r & Honest(RCAY) @i & r < i)"

////////////////////////////////COMMUNICATION


lemma there_willbe_orwas_an_EV_that_contacted_RCA:
exists-trace
"Ex EV RCA RandomnumberEV #i #j. Send(EV,RandomnumberEV)@i & Recv(RCA,RandomnumberEV) @j"


lemma There_Is_At_SomePoint_a_communication_between_EV_and_SECC:
exists-trace
"Ex EV SECC Id_Cert #i #j.
Send(EV, Id_Cert) @i
& Recv(SECC, Id_Cert) @j "

lemma there_willbe_orwas_a_SECC_that_contacted_RCA:
exists-trace
"Ex SECC RCA RandomnumberSECC #i #j. Send(SECC,RandomnumberSECC)@i & Recv(RCA,RandomnumberSECC) @j"
```

Figure 15 Quelques lemmes définis sur Tamarin Prover

5.2. Outils de simulation

5.2.1. Eclipse

Éclipse est un environnement de développement intégré (IDE) pour le langage de programmation Java ainsi que d'autres langages de programmation comme C/C++, Python, PERL, Ruby, etc. La plate-forme Éclipse, qui sert de base à l'IDE Éclipse, est composée de plug-ins et peut être étendue en ajoutant de nouveaux plug-ins. Cet IDE a été créé à l'aide de Java et peut être utilisé pour créer des environnements de développement intégré, des applications client et d'autres outils. Chaque langage de programmation pour lequel un plug-in est disponible peut être utilisé comme IDE avec Éclipse.

5.2.2. RISEV2G

Développé par Marc Mültin [35], RISE V2G est l'implémentation initiale qui prend en charge l'évolution de l'interface de communication Vehicle-2-Grid. ISO 15118 qui est la norme internationale intitulée « Road vehicles - network vehicle communication interface » définit une interface de communication numérique basée sur le protocole IP entre un VE et une borne de recharge (EVSE). RISEV2G permet un mécanisme convivial Plug And Charge (PnC) pour l'authentification, l'autorisation, la facturation et le contrôle de charge flexible basé sur un large ensemble d'informations échangées entre le VE et l'EVSE. Une augmentation de l'application à grande échelle de cette norme est essentielle pour atteindre l'objectif d'intégrer les véhicules électriques en tant que dispositifs de stockage d'énergie flexibles dans un réseau intelligent [36].

5.2.3. Virtual Box

VirtualBox est un puissant produit de virtualisation x86 et AMD64/Intel64 pour les entreprises et les particuliers. Non seulement VirtualBox est un produit extrêmement riche en fonctionnalités et hautes performances pour les clients d'entreprise, mais c'est aussi la seule solution professionnelle disponible gratuitement en tant que logiciel Open Source selon les termes de la licence publique générale GNU (GPL) version 3 [37].

5.2.4. Kali linux

Kali Linux (anciennement connu sous le nom de BackTrack Linux) est une distribution Linux open source basée sur Debian destinée aux tests de pénétration avancés et à l'audit de sécurité. Pour ce faire, il fournit des outils, des configurations et des automatisations communs qui permettent à l'utilisateur de se concentrer sur la tâche à accomplir, et non sur l'activité environnante.

Kali Linux contient des modifications spécifiques à l'industrie ainsi que plusieurs centaines d'outils ciblés sur diverses tâches de sécurité de l'information, telles que les tests d'intrusion, la recherche sur la sécurité, l'informatique juridique, l'ingénierie inverse, la gestion des vulnérabilités et les tests de l'équipe rouge. [38]

5.2.5. Wireshark

Wireshark est un analyseur de paquets réseau, qui présente les données de paquets capturées avec autant de détails que possible. C’est un analyseur de paquets réseau considéré comme un appareil de mesure pour examiner ce qui se passe lors des échanges.

Dans le passé, ces outils étaient soit très coûteux, soit propriétaires, soit les deux. Cependant, avec l'avènement de Wireshark, cela a changé. Wireshark est disponible gratuitement, il est open source et est l'un des meilleurs analyseurs de paquets disponibles aujourd'hui [39].

5.2.6. Ettercap

Ettercap est une suite complète pour des attaques de l'homme au milieu. Il propose une détection des connexions en direct, un filtrage de contenu et de nombreuses autres astuces intéressantes. Il prend en charge la dissection active et passive de nombreux protocoles et comprend de nombreuses fonctionnalités pour l'analyse du réseau et de l'hôte [40].

5.2.7. Méthodologie

Afin de valider notre proposition de protocole de PKI multi domaine pour les réseaux V2G, nous avons dû faire des simulations. Ces simulations ont été divisées en deux parties.

5.2.7.1. Partie 1

Nous avons créé plusieurs domaines (machines) avec l'outil virtuel box. Ensuite, nous avons lancé une session de chargement d'un VE et la borne qui sont dans le domaine 1, domaine 2 respectivement. À noter que chaque domaine a l'implémentation du simulateur open source RISEV2G que nous avons défini précédemment.

Pour expliquer l'idée de notre modèle, on doit d'abord comprendre comment les certificats fonctionnent dans Java et plus précisément sur Éclipse. Les certificats sur Java ont des notions très importantes, notamment :

- *KeyStore :* le Keystore contient des informations privées et sensibles, il est utilisé pour stocker la clé privée et les certificats d'identité qu'une entité spécifique doit présenter aux deux parties (serveur ou client) pour vérification.
- *TrustStore :* contrairement au Keystore, Truststore ne contient pas d'informations privées et sensibles. Les certificats des autorités de certifications qui valident le certificat fourni par le serveur dans une connexion SSL sont stockés ici.
- *Keytool :* c'est un utilitaire de gestion de certificats inclus avec Java, il gère un magasin de clés (base de données) de clés cryptographiques, des chaînes de certificats X.509 et des certificats de confiance. La commande keytool nous permet de créer des certificats autosignés et d'afficher des informations sur le keystore.
- *OpenSSL :* est une boîte à outils robuste, de qualité commerciale et complète pour les protocoles Transport Layer Security (TLS) et Secure Sockets Layer (SSL). C'est aussi une bibliothèque de cryptographie à usage général.

En donnant la définition de la base des certificats sous Java, on peut maintenant passer à l'explication de notre implémentation. D'abord dans RiseV2G, il y a un Keystore/TrustStore pour un EVCC et un SECC. En se basant sur les étapes présentées à la figure 11, les certificats ont été créés, enchaînés et enregistrés aux emplacements appropriés dans le Keystore/TrustStore de chaque entité (EVCC/SECC). Cette démarche garantit la gestion sécurisée des certificats et permet leur utilisation dans les échanges de données entre les différents composants du système.

Voici un exemple pour créer un certificat d'AC racine autosigné :

La figure 16 montre la période de validité des différents certificats recommandés par ISO15118 en jours.

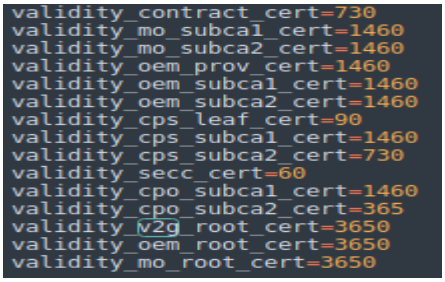

Figure 16 Période de validité des différents certificats recommandés par ISO15118

5.2.7.1.1. Créer une clé privée

- Clé privée -> -genkey
- Paramètres de courbe elliptique -> ecparam
- En utilisant la courbe nommée prime256v1 -> -name prime256v1
- Chiffrer la clé avec le chiffrement symétrique AES-128-CBC à l'aide de la commande utilitaire 'ec' -> ec -aes-128-cbc
- La phrase secrète pour le chiffrement de la clé privée est fournie dans un fichier -> -passout file : passphrase.txt
- Enregistrer la clé privée chiffrée à l'emplacement fourni -> -out

5.2.7.1.2. Créer une demande de signature du certificat (CSR)

- New -> - nouveau
- Demande de signature du certificat -> req
- En utilisant la clé privée créée précédemment à partir de laquelle la clé publique peut être dérivée -> -key

- Utiliser le mot de passe stocké dans le fichier pour déchiffrer la clé privée -> -passin
- Prend les valeurs nécessaires pour le Distinguished Name (DN) du fichier de configuration -> -config
- Enregistre le CSR à l'emplacement indiqué -> -out

5.2.7.1.3. Créer un certificat X.509

- Utiliser la commande de l'utilitaire X.509 -> x509
- Demande d'un nouveau certificat X.509 ... -> -req
- En utilisant un fichier CSR qui se trouve à -> -in
- Nous avons besoin d'un certificat X.509v3 (version 3) qui autorise les extensions. Ceux-ci sont spécifiées dans un fichier d'extensions... -> -extfile qui contient une section marquée par 'ext' -> -extensions
- Auto-signer le certificat avec la clé privée précédemment générée -> -signkey
- Utiliser le mot de passe stocké dans le fichier pour déchiffrer la clé privée -> -passin
- Indiquer à OpenSSL d'utiliser SHA-256 pour créer la signature numérique (sinon SHA1 serait utilisé) -> -sha256
- Chaque certificat émis doit contenir un numéro de série unique attribué par l'AC (doit être unique dans la plage de numéros des émetteurs) -> -set_serial
- Enregistrer le certificat à l'emplacement indiqué -> -out
- Rendre le certificat valable 40 ans (donné en jours) -> -days. (Voir Fig.17)

```
openssl ecparam -genkey -name prime256v1 openssl ec -aes-128-cbc -passout
 file:passphrase.txt -out privateKeys/v2gRootCa.keystores

 openssl req -new -key privateKeys/v2gRootCA.key -passin file:passphrase.txt
 -config configs/v2gRootCACert.cnf -out csrs/v2gRootCA.certs


 openssl x509 -req -in csrs v2gRootCA.csr -extfile configs/v2gRootCACert.cnf -extentions
 ext -signkey privateKeys/v2gRootCA.key -passin file:passphrase.txt
 -sha256 -set_serial 123456 -out certs/v2gRootCACert.pem -days $validity_v2g_roo_cert
```

Figure 17 Création du certificat ROOT V2G auto signé

On crée tous les certificats cités dans la figure 11 de la mème manière, notamment :

- Certificat racine V2G
  - Certificat d'approvisionnement intermédiaire 1.
  - Certificat d'approvisionnement intermédiaire 2.
  - Certificat d'approvisionnement.
- Certificat Opérateur de bornes de recharge (CPO)
  - Certificat intermédiaire CPO 1.
  - Certificat intermédiaire CPO2.
  - Certificat SECC.
- Certificat racine d'opérateur de mobilité (OM).
  - Certificat intermédiaire OM 1.
  - Certificat intermédiaire OM 2.
  - Certificat de contrat.
- Certificat racine original Equipment manufacturer (OEM).
  - Certificat intermédiaire OEM 1.
  - Certificat intermédiaire OEM 2.
  - Certificat d'approvisionnement OEM.

5.2.7.1.4. Cross certification

Par définition [30] et selon la méthodologie suivie dans le chapitre IV phase 1, l'AC racine du domaine 1 signe la clé publique de l'AC racine de domaine 2 et diffuse ses informations à son domaine respectif en étant un ancrage de confiance, et vice-versa.

5.2.7.1.4.1. Signature de la clé publique.

L'AC racine du premier domaine signe avec sa clé privée l'AC racine du deuxième domaine. (Voir Fig.18)

```
openssl ec -in privateKeys/v2gRootCA.key -pubout -out publicKeys/v2gRootCA1Publickey.pem

openssl dgst -sha1 -sign privateKeys/v2gRootCA.key -out
publicKeys/v2gRootCA2Publickey.sign ../vmRise/RISE-V2G-master/RISE-V2G-Certificates/publicKeys/v2gRootCA2Publickey.pem
```

Figure 18 Root AC1 signe Root AC2

Ensuite, le deuxième domaine signe l'AC racine du premier domaine. (Voir Fig.19)

```
openssl ec -in privateKeys/v2gRootCA.key -pubout -out publicKeys/v2gRootCA2Publickey.pem

 openssl dgst -sha1 -sign privateKeys/v2gRootCA.key -out
 publicKeys/v2gRootCA1Publickey.sign ../../../RISE-V2G-Certificates/publicKeys/v2gRootCA1Publickey.pem
```

Figure 19 Root AC2 signe Root AC1

5.2.7.1.4.2. Diffusion des informations comme étant un ancrage de confiance.

L'EVCC doit obligatoirement avoir le certificat V2G racine de son domaine et comme les deux AC viennent de faire une cross certification, l'EVCC du premier domaine doit avoir le certificat V2G racine de son domaine et ainsi le certificat V2G racine de l'autre domaine. Ce qui implique le code OpenSSL sur la figure 20 :

```
keytool -import -keystore keystores/evccTruststore.jks
 -alias v2g_root_ca -file certs/v2gRootCACert.der
  -storepass:file passphrase.txt -noprompt

keytool -import -keystore keystores/evccTruststore.jks
-alias v2g_root_ca2 -file ../vmRise/RISE-V2G-master/RISE-V2G-Certificates/certs/v2gRootCACerts.der
 -storepass:file passphrase.txt -noprompt
```

Figure 20 Diffusion de l'ancrage de confiance 1 Keystore du VE du domaine 1

La même chose pour domaine 2, son EVCC doit avoir les deux V2G root Certificat :

```
keytool -import -keystore keystores/evccTruststore.jks
 -alias v2g_root_ca -file certs/v2gRootCACert.der
  -storepass:file passphrase.txt -noprompt

keytool -import -keystore keystores/evccTruststore.jks
-alias v2g_root_ca2 -file ../../../RISE-V2G-Certificates/certs/v2gRootCACerts.der
 -storepass:file passphrase.txt -noprompt
```

Figure 21 Diffusion de l'ancrage de confiance 2 Keystore du VE du domaine 2

Dans le cas de SECC, son TrustStore doit avoir le certificat racine V2G et le certificat racine d'OM. Ainsi, la borne fait confiance au EVCC lorsque celui-ci lui envoie son certificat grâce à une succession de signatures. Effectivement, le certificat du EVCC provient du certificat racine d'OM d'où l'enchainement des signatures qui débute. Le certificat racine d'OM signe l'OM sub AC1 *(certificat intermédiaire OM 1)* qui signera à son tour l'OM sub AC2 *(certificat intermédiaire OM 2)*.

Au final, le certificat d'EVCC obtient sa signature d'OM sub AC2 et peut ainsi se connecter à la borne de recharge qui lui fera confiance. Ceci étant dit, le SECC doit avoir une chaine de confiance valide jusqu'à l'ancrage de son domaine et de son

ancrage de confiance de deuxième domaine qui sont dans ce cas : *certificat racine V2G* et *certificat racine d'OM* **(des deux domaines).** L'addition du certificat racine d'OM n'est pas obligatoirement nécessaire dans le TrustStore de SECC car selon la norme ISO15118, OM sub AC1 peut être signé par le certificat racine V2G [5] (voir figure 11). La figure 22 montre l'implémentation de cette étape.

```
keytool -import -keystore keystores/seccTruststore.jks -alias v2g_root_ca -file certs/v2gRootCACert.der
-storepass:file passphrase.txt -nonprompt

keytool -import -keystore keystores/seccTruststore.jks -alias v2g_root_ca2
-file ../vmRise/RISE-V2G-master/RISE-V2G-Certificates/certs/v2gRootCACert.der
-storepass:file passphrase.txt -nonprompt


#Mobility_operator

keytool -import -keystore keystores/seccTruststore.jks -alias mo_root_ca -file certs/moRootCACert.der
-storepass:file passphrase.txt -nonprompt
keytool -import -keystore keystores/seccTruststore.jks -alias mo_root_ca2
-file ../vmRise/RISE-V2G-master/RISE-V2G-Certificates/certs/moRootCACert.der
-storepass:file passphrase.txt -nonprompt
```

Figure 22 Création de Trust Store de domaine 1

De même, la figure 23 montre la création de Truststore de SECC de Domaine 2.

```
keytool -import -keystore keystores/seccTruststore.jks -alias v2g_root_ca -file certs/v2gRootCACert.der
-storepass:file passphrase.txt -nonprompt

keytool -import -keystore keystores/seccTruststore.jks -alias v2g_root_ca2
-file ../../../RISE-V2G-Certificates/certs/v2gRootCACert.der
-storepass:file passphrase.txt -nonprompt


#Mobility_operator

keytool -import -keystore keystores/seccTruststore.jks -alias mo_root_ca -file certs/moRootCACert.der
-storepass:file passphrase.txt -nonprompt
keytool -import -keystore keystores/seccTruststore.jks -alias mo_root_ca2
-file ../../../RISE-V2G-Certificates/certs/moRootCACert.der
-storepass:file passphrase.txt -nonprompt
```

Figure 23 Création de Trust Store de domaine 2

5.2.7.2. Partie 2

La deuxième partie consiste à mesurer la performance de notre modèle sous les attaques. Pour cela, nous allons faire subir à notre modèle plusieurs attaques réseau sous Kali Linux. Il sera installé dans une autre machine virtuelle à l'aide de VirtualBox. Avec Kali Linux, en utilisant les outils Wire Shark et Ettercap présentés précédemment. (Voir Fig.24)

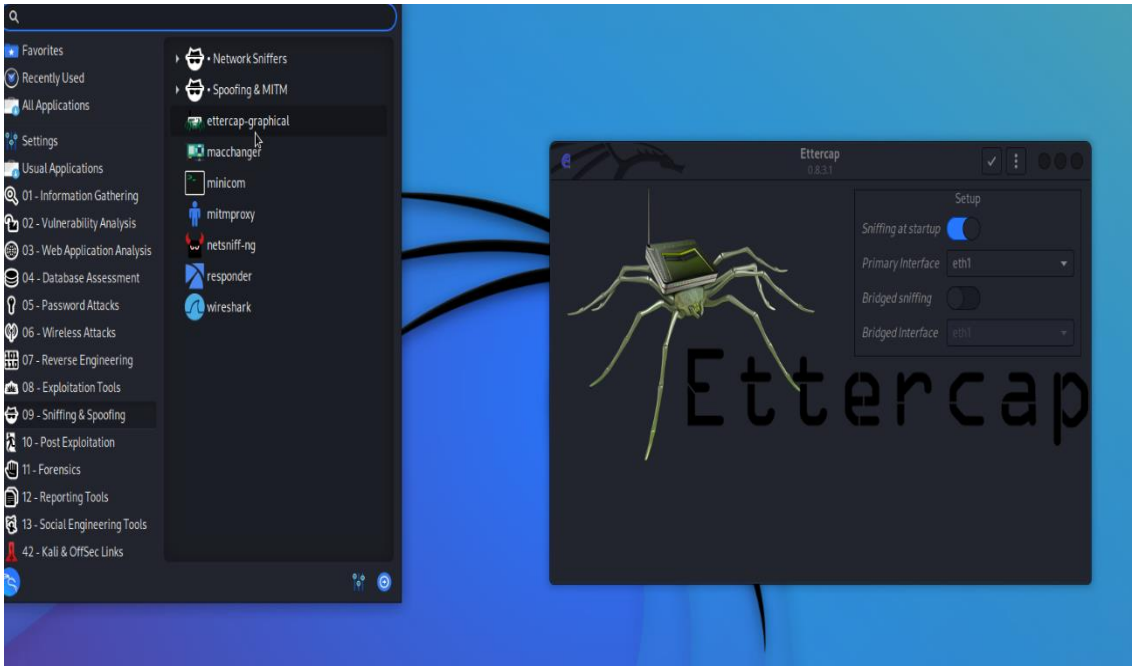

Figure 24 Interface Graphique de l'outil Ettercap

Notre modèle a subi différents types d'attaques d'hommes du milieu dans le but d'évaluer son efficacité. Parmi les attaques utilisées on a :

- Empoisonnement d'ARP
- Redirection d'ICMP,
- Vol du SSL
- Wire Shark.

Enfin, puisque notre modèle supporte l'intra domaine comme la version standard et inter domaine également (multi Domaine), nous avons comparé le niveau des paquets interceptés de notre protocole avec ISO15118 car pour autant que nous sachions à ce jour, il n'y a pas eu de simulation d'un PKI multi domaine pour un réseau V2G que nous pourrions comparer à notre protocole.

Chapitre VI

Résultats de modélisation et de simulation

Dans ce qui suit nous allons présenter les résultats obtenus grâce à la modélisation faite à l'aide de l'outil de Tamarin Prover et ensuite les résultats de la simulation de notre protocole sous le simulateur riseV2G avec les attaques que nous avons implémentées afin de valider l'efficacité de notre proposition.

6.1. Résultats de modélisation

Les résultats donnés par Tamarin Prover nous ont permis de conclure que notre protocole est très opérationnel. À partir des lemmes proposés, nous pouvons dire que notre protocole assure la confidentialité, l'intégrité et la non-répudiation des informations transmises entre les entités du réseau V2G. tel qu'on peut le voir à la figure 25.

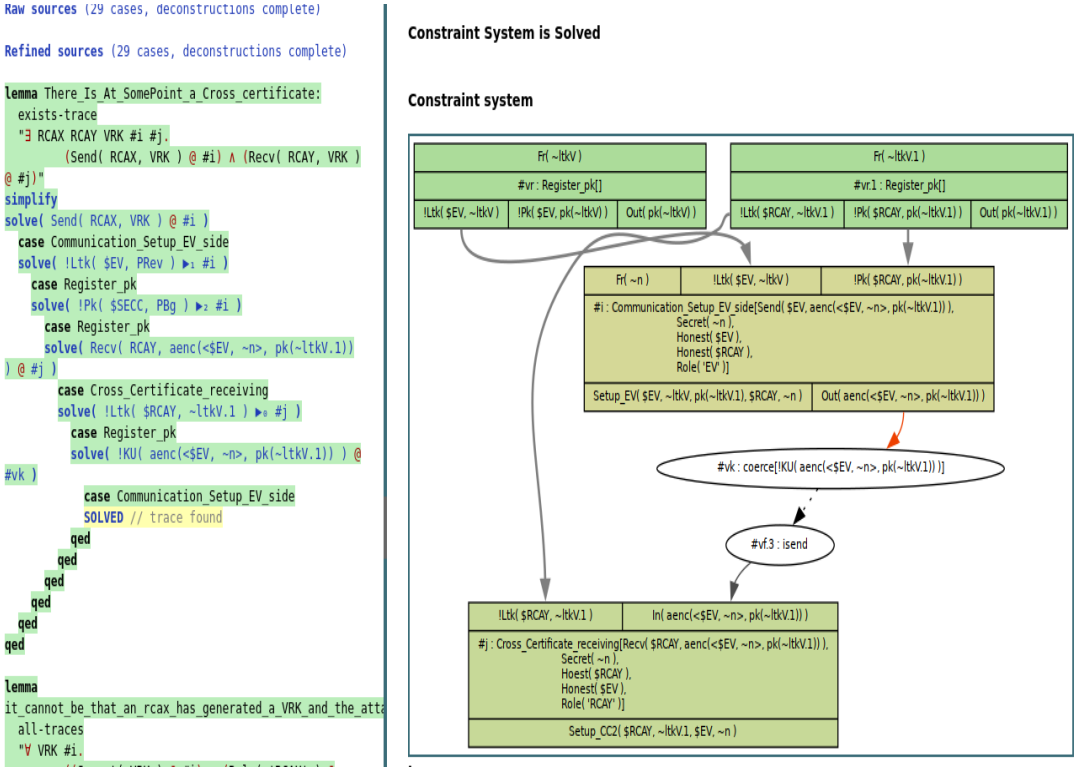

Figure 25 Résultat de modélisation

6.2. Résultats de simulation

6.2.1. Partie 1

Tout d'abord nous avons commencé la première partie en simulant une session de charge avec le standard de la norme ISO15118 dans deux domaines. Les résultats montrent un échec de l'établissement de la communication en raison d'un *mauvais certificat*, un *échec du chemin de validation* et ainsi un *échec de contrôle de signature* comme on peut le voir à la figure 26.

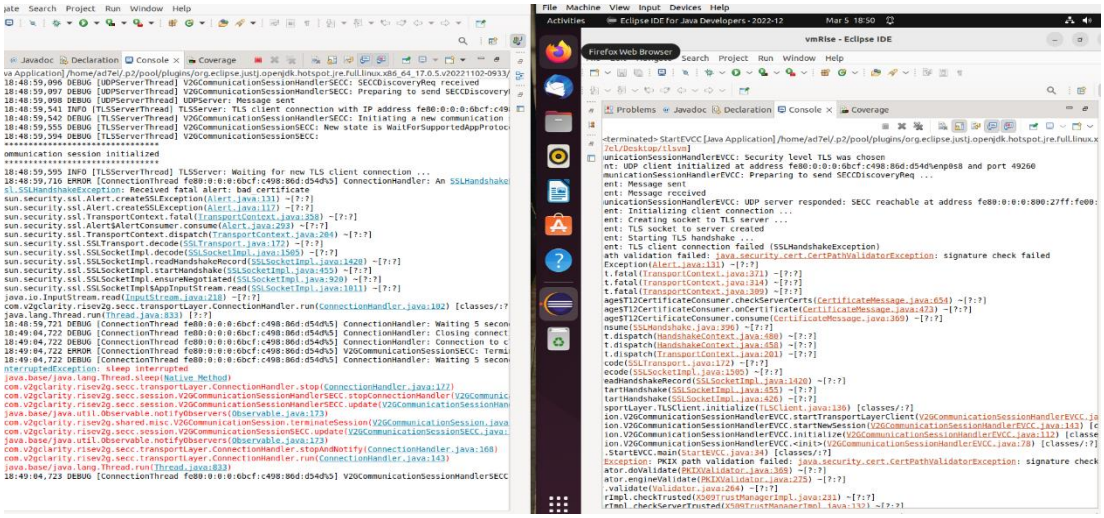

Figure 26 Session de communication multi domaine avec le standard ISO15118

Cet échec montre que la norme ne prend pas en charge l'infrastructure PKI multi domaine. Cependant, l'application de notre modèle sous riseV2G établit avec succès une session de charge sécurisée qui a fait qu'un VE dans le domaine 1

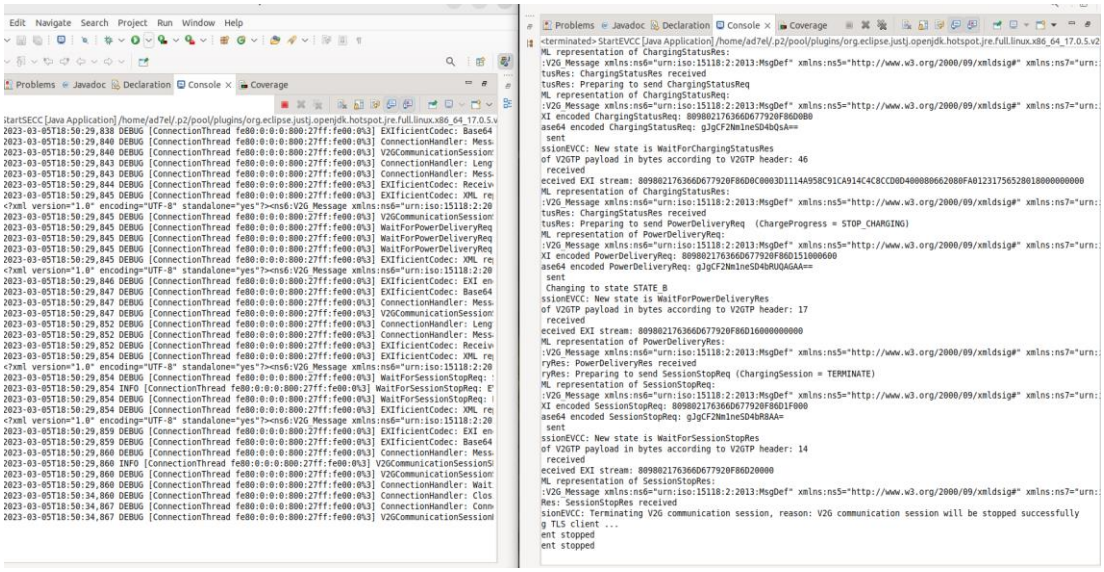

Figure 27 Session de communication multi domaine avec notre Protocole

communique en toute sécurité avec un SECC dans le domaine 2 (voir figure 27). De plus, notre modèle peut également établir une session de charge avec un SECC dans son domaine par défaut.

6.2.2. Partie 2

6.2.2.1. Résultat d'attaques

- Empoisonnement d'ARP

La première étape pour effectuer un empoisonnement ARP est de scanner les hôtes qui sont connectés à une interface précise qu'on trouve à l'ouverture du logiciel Ettercap. Après avoir scanné les hôtes, on fixe des victimes, comme on peut le voir à la figure 28 en haut à droite (target.1 and target.2).

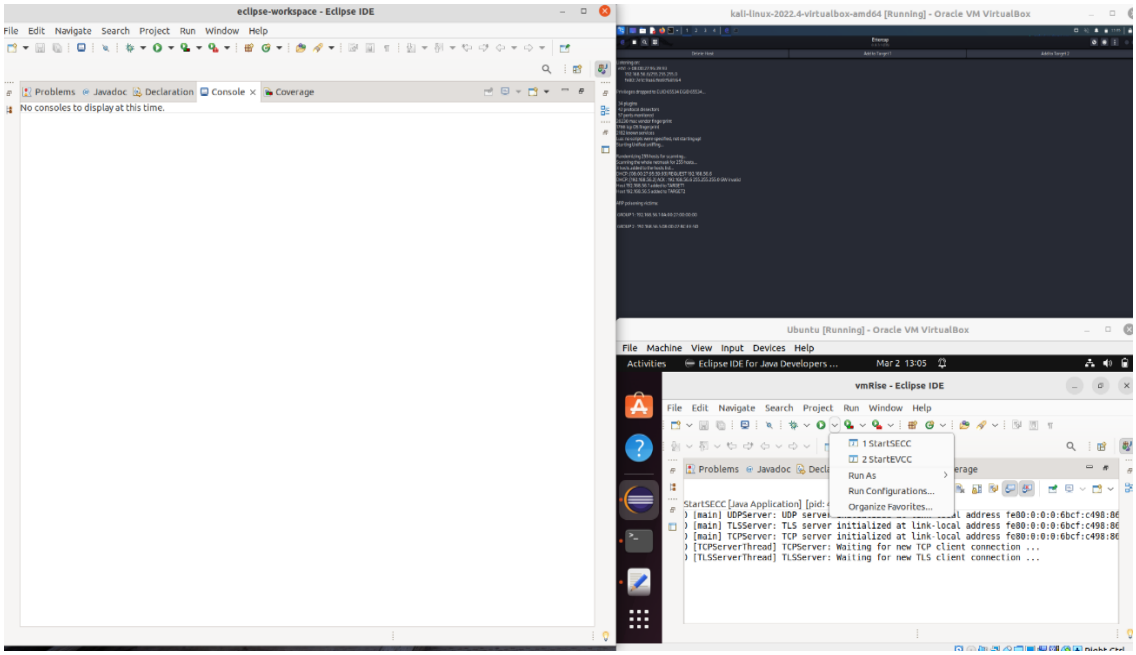

Figure 28 Préparation de l'attaque d'empoisonnement ARP en utilisant Ettercap.

En bas à droite de la figure 29, on lance la borne (SECC) et à gauche, on lance le VE (EVCC). La figure 29 montre qu'une session de chargement a été terminé avec succès sans que l'empoisonnement ARP ne puisse créer des vulnérabilités sur la session de communication.

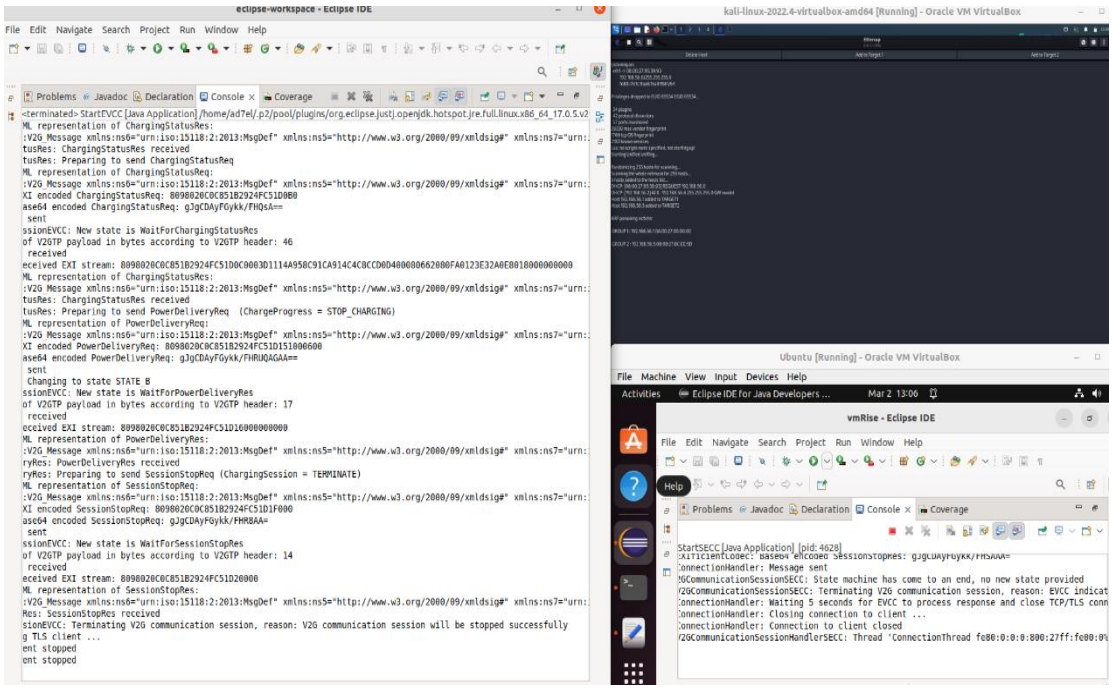

Figure 29 Résultats de l'attaque d'empoisonnement ARP

- Redirection d'ICMP

Avec la redirection d'ICMP, on a besoin de l'adresse IP et de l'adresse MAC du véhicule ciblé. On saisit ses informations dans l'interface comme on peut le voir à la figure 30 en haut à droite et on lance de nouveau une session de communication pour le chargement. En résultat, on peut voir en bas à gauche que la session s'est terminée avec succès.

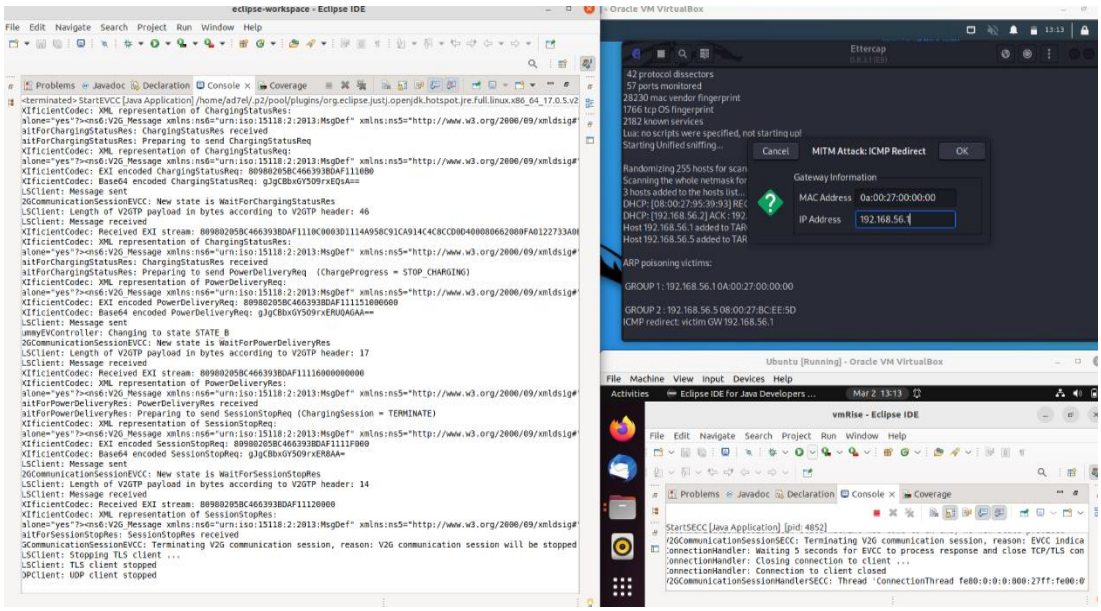

Figure 30 Résultats de l'attaque de redirection d'ICMP

- Vol du SSL

Afin d'appliquer une attaque de type vol du SSL, on doit activer SSL Strip sur l'outil Ettercap comme on peut le voir au niveau de la figure 31. On laisse l'empoisonnement ARP s'activer sur les deux cibles et on lance une session de communication. On remarque dans la figure que notre protocole effectue une session de chargement sans capturer les paquets TLS ou n'importe quel autre paquet sensible ou risque de contenir des données sensitives.

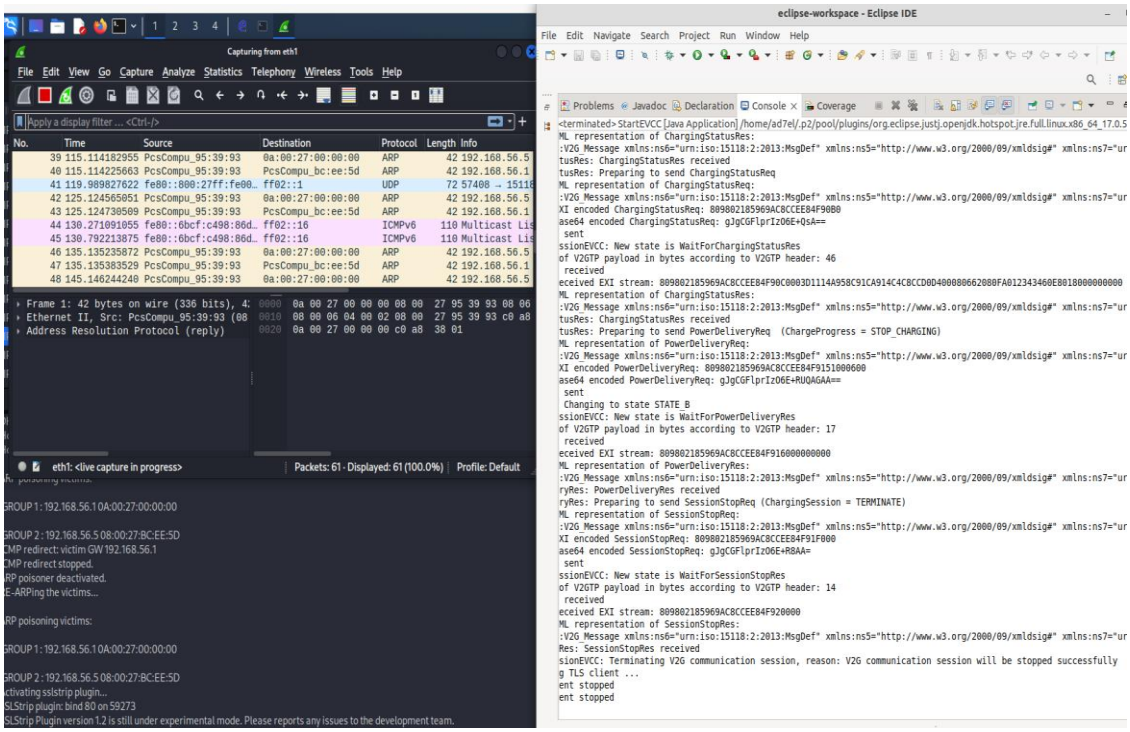

Figure 31 Résultats de l'attaque de Vol du SSL

En résumant, nous avons utilisé des outils de détection et d'usurpation d'identité dans Kali Linux pour effectuer plusieurs attaques d'homme au milieu, en particulier avec Ettercap. Notre protocole est efficace contre l'empoisonnement ARP, la redirection d'ICMP et le vol du SSL.

6.2.2.2. Comparaison des Interception de paquets

Dans le cas des paquets interceptés, pour pouvoir faire une comparaison entre notre modèle et le modèle standard, 100 sessions de charge ont été évaluées avec l'outil Wire Shark. L'idée est de lancer une session de communication et voir de ce qu'il peut intercepter. À la figure 32, nous avons comparé le niveau d'interception de paquets que l'outil Wireshark peut capturer durant 100 sessions de communication (entre l'EVCC et SECC) entre le protocole standard et notre protocole.

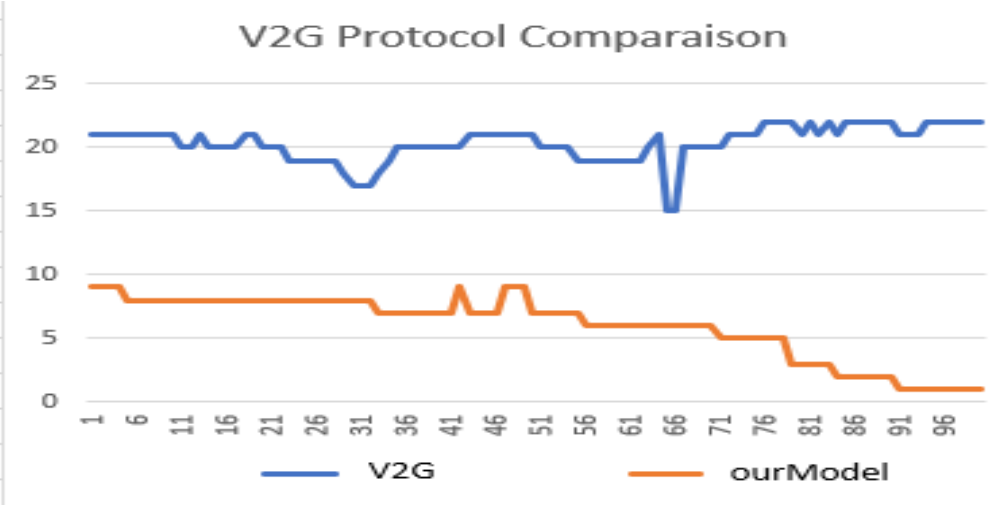

Figure 32 Comparaison d'interception de paquets entre notre modèle et le modèle standard V2G

La comparaison entre la ligne bleue, représentant le protocole standard intercepté par l'outil Wireshark, et la ligne orange, représentant notre modèle, met en évidence une différence significative. Alors que le protocole standard permet d'intercepter jusqu'à 20 paquets par session de charge, ce qui présente un risque élevé pour la sécurité des informations sensibles, notre modèle se limite à seulement 5 paquets par session. De plus, ces paquets sont de nature UDP et ARP et ne constituent aucune menace pour la sécurité de la communication. Ainsi, notre modèle offre une meilleure protection et réduit considérablement les risques liés à l'interception de paquets.

6.3. Analyse pratique de la sécurité

Dans ce chapitre, notre objectif était de présenter un modèle de sécurité solide pour le système V2G multi domaine. Afin d'assurer la robustesse et la fiabilité de ce

modèle, une analyse pratique de la sécurité a été entreprise, Voici comment les aspects de confidentialité et d'authentification, d'intégrité, de non-répudiation et d'anonymat ont été assurés :

Confidentialité : La clé privée générée est chiffrée avec le chiffrement symétrique AES-128-CBC. Cela assure la confidentialité de la clé privée, car elle ne peut être déchiffrée qu'avec la *Passphrase* spécifiée dans le fichier.

Authentification : L'utilisation de la *Passphrase* pour chiffrer la clé privée ajoute une couche de protection supplémentaire. Lors de la création du certificat X.509, la clé privée précédemment générée est utilisée pour signer le certificat. Cela garantit l'authenticité du certificat, car il est signé avec la clé privée correspondante.

Intégrité : Lors de la création du certificat X.509, OpenSSL utilise le hachage SHA-256 pour créer la signature numérique du certificat. Cela garantit l'intégrité du certificat, car toute modification apportée au certificat entraînerait une invalidation de la signature.

Non-répudiation : En utilisant une clé privée pour signer le certificat X.509, on assure la non-répudiation. Une fois que le certificat est signé avec la clé privée, il ne peut pas être nié ultérieurement par la partie qui l'a signée.

Anonymat : L'utilisation de pseudo-entités, telles que les pseudonymes générés par OpenSSL lors de la création des clés privées et des certificats X.509, permet de préserver l'anonymat des entités impliquées dans les échanges. En utilisant ces pseudo-entités, les véritables identités des entités sont dissimulées, renforçant ainsi la confidentialité des données personnelles des entités.

L’analyse pratique de la sécurité de notre modèle a démontré l'importance cruciale d'une approche complète et rigoureuse en matière de sécurité. Les points examinés, tels que la confidentialité, l'authentification, l'intégrité, la non-répudiation

et l'anonymat, ont été soigneusement pris en compte pour garantir la solidité et la fiabilité du notre modèle de sécurité. Grâce à ces mesures et à leur mise en œuvre efficace, le système V2G multi domaine peut fonctionner de manière sécurisée et protéger les données sensibles des utilisateurs, tout en maintenant leur confiance dans l'ensemble du processus d'échange.

6.4. Conclusion

Nous nous sommes concentrés dans ce chapitre sur les aspects de modélisation et de simulation de notre recherche. Nous avons utilisé divers outils à cette fin. Tamarin Prover a été utilisé pour la vérification formelle de notre protocole, Eclipse a servi d'environnement de développement intégré et RISE V2G a facilité les simulations de sessions de communication. De plus, Kali Linux a été utilisé pour mener des simulations d'attaques, Wireshark a aidé à l'analyse des paquets réseau et Ettercap a pris en charge les attaques de type man-in-the-middle. Ces outils ont été soigneusement sélectionnés pour leur compatibilité avec les réseaux V2G. Les simulations et les efforts de modélisation étaient essentiels pour évaluer les performances et la sécurité de notre protocole PKI multi-domaine proposé pour les réseaux V2G. Grâce à ces simulations, nous avons pu démontrer que notre approche était faisable, solide et elle répond à toutes les exigences de sécurité.

Chapitre VII

Conclusion et perspective futurs

L’utilisation croissante des véhicules électriques dans les années à venir nécessitera un déploiement à grande échelle de l'infrastructure V2G, Une infrastructure qui doit être sûre contre les vulnérabilités. D’où la nécessité de définir et implémenter une architecture mondiale sécurisée, robuste et évolutive.

Notre état de l’art sur les protocoles de communication dans les réseaux V2G nous a permis d’étudier l’existant et d’analyser avec les besoins, les points forts et faibles des solutions existantes et d’améliorer leurs limites et défauts.

Dans le cadre de ce mémoire, nous avons proposé un protocole de communication sécurisé qui prend en charge la communication inter et intra domaine dans les réseaux V2G. Outre cela, et au mieux de nos connaissances, ce protocole couvre les fondamentaux de la sécurité informatique les plus importants tels que la confidentialité, l'intégrité, l'anonymat, la non-répudiation avec l’authentification mutuelle qui est implémenté au niveau des deux parties de communication qui sont le véhicule électrique et la borne de recharge.

La modélisation de notre protocole sous Tamarin Prover et la simulation avec l’outil RiseV2G sous des attaques d’homme du milieu nous a permis de certifier et valider l'efficacité de notre solution. Les simulations réalisées nous ont montré que l'extension de la limitation de l'ISO15118 qui ne prend pas en charge l’infrastructure PKI multi domaine est possible. De plus, il a également été démontré que notre protocole est moins vulnérable aux attaques qui ciblent la confidentialité, la non-répudiation et l'intégrité des données.

L’avenir des réseaux V2G repose sur plusieurs axes stratégiques. Tout d'abord, l'élaboration de normes internationales cohérentes et harmonisées facilitera l'interopérabilité et renforcera la sécurité des transactions V2G à l'échelle mondiale. Ensuite, l'optimisation de la gestion de la charge des véhicules électriques permettra de mieux équilibrer la demande énergétique et de maximiser l'utilisation des

ressources. De plus, L'intégration avec les réseaux intelligents permettra une coordination efficace entre les sources d'énergie distribuées, les dispositifs de stockage et les charges électriques, contribuant ainsi à une meilleure qualité de service et à l'efficacité énergétique. Enfin, des mesures de sécurité avancées, telles que l'authentification robuste, le chiffrement des données et la résilience face aux cyberattaques, seront essentielles pour protéger les réseaux V2G et instaurer la confiance des utilisateurs. Ce travail peut être étendue et perfectionnée par l'intégration fluide des réseaux V2G aux réseaux électriques intelligents, favorisant ainsi une coordination optimisée entre les sources d'énergies renouvelables. L'idée est de compléter ce travail en intégrant la solution aux acteurs secondaires qui font parties et du réseau V2G et de la grille intelligente.

Cette perspective d'avenir contribuera à un déploiement plus large et sécurisé des véhicules électriques, favorisant ainsi l'accomplissement d'un système énergétique sécuritaire, efficient, durable et de qualité.

Bibliographie

[1] I. E. Agency, «International Energy Agency,» International Energy Agency, Global EV Outlook 2022, 05 2022. [En ligne]. Available: https://www.iea.org/data-and-statistics/data-product/global-ev-outlook-2022#. [Accès le 19 12 2022].

[2] F. S.-L. e. S.-P. R. Jean-François Morissette, «Quebec Electric Vehicle Association,» Quebec Electric Vehicle Association, 2023 02 11. [En ligne]. Available: https://www.aveq.ca/actualiteacutes/statistiques-saaq-aveq-sur-lelectromobilite-au-quebec-en-date-du-31-decembre-2022-infographie. [Accès le 2023 03 03].

[3] Y. F. Z. ,. H. Q. S. J. Sun, « An efficient distributcd kcy management scheme for group-signature based anonymous authentication in VANET. Security And Communication Networks,» pp. 79-86, 05 2012.

[4] A. BELKAALOUL, *DÉVELOPPEMENT D'UNE INFRASTRUCTURE À CLÉS PUBLIQUES POUR,* Trois Riviere: Université de quebec a Trois Riviere, 2021.

[5] I. O. f. Standardization, «. Road vehicles - Vehicle to grid communication Interface ISO15118,» Switzeland, 2014.

[6] B. M. D. &. M. H. Vaidya, «Effective public key infrastructure for vehicle-to-grid network.,» *Proceedings Of Th e Fourth ACM International Symposium On Development And Analysis Of Intelligent Vehicular Networks And Applications,* pp. 95-101, 2014.

[7] T. K. D. ,. C. P. Fran Casino, «A systematic literature review of blockchain-based applications:,» *Telematics and Informatics, elsevier,* vol. 36, pp. 55-81, 2019.

[8] e. A. F. A. G. S. A. J. K. aysha albarqi, «public key infrastructure: A survey,» *journal of information security,* vol. 6, pp. 31-37, 2015.

[9] R. A. R. P. M. S. P. Varsharani hawanna V Y. Kulkarni, « Risk Rating system of X.509 certificate,» *Procedia Computer science, Elsevier,* vol. 89, pp. 152-161, 2016.

[10] P. K. M. B. Balachandra Muniyal, «COMPARISON OF CERTIFICATE POLICIES FORMERGING PUBLIC KEY INFRASTRUCTURESDURING,» *International Journal of Network Security & Its Application,* vol. 4, n° %15, 2012.

[11] H. E. B. Zakia EL UAHHABI, «A Comparative Study of PKI Trust Models,» *2014 Fifth International Conference on Next Generation Networks and Services (NGNS) ,* 28-30 05 2014.

[12] H. K.-A. Paul Danquah, «Public Key Infrastructure: An Enhanced Validation Framework,» *Journal of Information Security ,* vol. 11, n° %104, 2020.

[13] B. S. Prosanta Gope, «An Efficient Privacy-Preserving Authentication Scheme for

Energy Internet-Based Vehicle-to-Grid Communication,» *IEEE Transactions on Smart Grid,* vol. 10, n° %16, 2019).

[14] G. S. M. Z. Yixin Su, «A Novel Privacy-Preserving Authentication Scheme for V2G Networks,» *IEEE Systems Journal,* vol. 14, n° %12, pp. 1963 - 1971, June 2020.

[15] D. O.-S. A. M. S. N. M. Abbasinezhad-Mood, «Provably-secure escrow-less Chebyshev chaotic map-based key agreement protocol for vehicle to grid connections with privacy protection,» *IEEE Transactions on Industrial Informatics (,* vol. 16, n° %112, pp. 7287 - 7294, December 2020.

[16] S. L. M. Mu Han, «Anonymous-authentication scheme based on fog computing for VANET,» 2020.

[17] N. V. C. B. S. N. K. M. G. Gaurang Bansal, «Lightweight mutual authentication protocol for V2G using physical unclonable function,» *IEEE Transactions on Vehicular Technology ,* vol. 69, p. 7234–7246, 2020.

[18] D. M. M. R. M. Masoud Kaveh, «A Lightweight Authentication Scheme for V2G Communications: A PUF-Based Approach Ensuring Cyber/Physical Security and Identity/Location Privacy,» *Electronics,* 2020.

[19] G. D. J. P. M. A. P. Merlinda Andoni Valentin Robu David Flynn Simone AbramDale, «Blockchain technology in the energy sector: A systematic review of of challenges and opportunities,» *Renewable and Sustainable Energy Reviews,* pp. 143-179, 2019.

[20] K. K. G. K. F. G. J. J. P. C. R. Sahil Garg, «An Efficient Blockchain-based Hierarchical Authentication Mechanism for Energy Trading in V2G environment,» *n IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China,* 20-24 May 2019.

[21] V. C. S. G. N. G. K. D. G. K. a. D. N. V. Hassija, «A blockchain-based framework for lightweight data sharing,» *IEEE Transactions on Vehicular Technology,* vol. 69, n° %16, p. 5799–5812, 2020.

[22] K. K. C. X. Z. E. L. a. C. Liu, «Adaptive blockchain based electric vehicle participation scheme in smart grid platform,» *IEEE access,* vol. 6, pp. 25657–25665, , 2018..

[23] L. L. A. S. Anjee Gorkhalia, «Blockchain: a literature review,» *Journal of Management Analytics,* vol. 7, n° %13, p. 321–343, 2020.

[24] S. G. K. F. S. K. Kaur, «Blockchain based lightweight authentication mechanism for vehicular fog infrastrucure,» *IEEE international conference on communication. workshops,* pp. 1-6, 2019.

[25] D. M. H. .. T. M. Binod Vaidya, «Multi-domain Public Key Infrastructure for Vehicle-to-Grid Network,» *IEEE Military Communications Conference,* pp. 1572-1577, octobre

2015.

[26] J. M. M. M. E. A. Mahmoud, «A Scalable Public Key Infrastructure for Smart grib communications,» *Globecom 2013 - Communication and Information System Security Symposium,* pp. 784-789, 2013.

[27] H. N. Y. Z. M. G. Hong Liu, «Battery Status-aware Authentication Scheme for V2G Networks in Smart Grid,» *IEEE TRANSACTIONS ON SMART GRID, VOL. 4, NO. 1, MARCH 2013,* vol. 4, n° %11, pp. 99-110, 2013.

[28] Z. F. ,. K. G. ,. J. W. ,. J. T. ,. G. W. Zhuoqun Xia, «Effective charging identity authentication scheme based on fog computing in V2G networks,» *Journal of Information Security and Applications ,* 2021.

[29] D. M. H. T. M. Binod Vaidya, «Security Mechanism for Multi-domain Vehicle-toGrid Infrastructure,» *IEEE Globecom 2011,* 2011.

[30] C. o. N. S. S. Instruction, «INSTRUCTION FOR SECRET NATIONAL SECURITY SYSTEMS PUBLIC KEY INFRASTRUCTURE X.509 CERTIFICATE POLICY,,» 2021.

[31] C. C. J. D. S. M. R. S. B. S. David Basin, «tamarin Prover,» github, [En ligne]. Available: https://tamarin-prover.github.io/. [Accès le 05 03 2023].

[32] C. Cremers, M. Horvat, S. Scott et T. van der Merwe, «Automated Analysis and Verification of TLS 1.3: 0-RTT, Resumption and Delayed Authentication". May 22-26, 2016.,» *IEEE Symposium on Security and Privacy, 2016, San Jose, CA, USA.,* pp. 470-485, 22-26 05 2016.

[33] D. Basin, C. Cremers et S. Meier, «Provably repairing the ISO/IEC 9798 standard for entity authentication.,» *Journal of Computer Security,* vol. 21, n° %16, p. 817–846, 2013.

[34] A. B. B. Abdallah Belkaaloul, «Anonymous Authentication Protocol for Efficient Communications in Vehicle to Grid Networks,» *2021 IEEE Symposium on Computers and Communications,* 2021.

[35] «eclipse foundation,» eclipse RISEV2G, [En ligne]. Available: https://projects.eclipse.org/projects/iot.risev2g/who. [Accès le 05 03 2023].

[36] «Github,» SwitchEV-MIT licence, [En ligne]. Available: https://github.com/SwitchEV/RISE-V2G. [Accès le 05 03 2023].

[37] oracle, «virtualBox,» oracle, [En ligne]. Available: https://www.virtualbox.org/. [Accès le 05 03 2023].

[38] g0tmi1k, «Kali linux,» Kali, 27 Sep 2022. [En ligne]. Available: https://www.kali.org/docs/introduction/what-is-kali-linux/. [Accès le 05 03 2023].

[39] G. Combs, «Wireshark,» Wireshark, [En ligne]. Available: https://www.wireshark.org/docs/wsug_html/#ChIntroWhatIs. [Accès le 05 03 2023].

[40] E. project, «Ettercap,» Ettercap , [En ligne]. Available: https://www.ettercap-project.org/index.html. [Accès le 05 03 2023].

[41] C. o. N. S. S. Instruction, «INSTRUCTION FOR SECRET NATIONAL SECURITY SYSTEMS PUBLIC KEY INFRASTRUCTURE X.509 CERTIFICATE POLICY,» 2021.

[42] oracle, «The Public Key Infrastructure Approach to Security.,» oracle , 2002. [En ligne]. Available: The Public Key Infrastructure Approach to Security.. [Accès le 03 03 2023].

[43] e. org, «eclipse org,» eclipse org, [En ligne]. Available: https://www.eclipse.org/ide/. [Accès le 05 03 2023].

[44] B. N. C. B. D. D. a. C. W. E. Mengelkamp, «A blockchain-based smart grid: Towards sustainable local energy markets,» *Computer Science - Research and Development,* vol. 33, n° %11-2, p. 207–214, 2018.

[45] F. L. Z. C. T. M. a. X. S. Xia, «A Bayesian game based vehicle-to-vehicle electricity trading scheme for blockchain-enabled internet of vehicules,» *IEEE Transactions on Vehicular Technology,* vol. 69, n° %17, pp. 6856–6868,, 2020.