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
SAIDOU DIOP

UNE INFRASTRUCTURE A CLES PUBLIQUES (PKI) POUR SECURISER LES MESSAGES DANS UN RESEAU V2G

MARS 2018

Remerciements

Je tiens en premier lieu à exprimer mes remerciements et ma profonde gratitude à mon encadrant, le Professeur Boucif Amar Bensaber, qui de par ses conseils et ses encouragements ainsi que le temps qu'il m'a consacré tout au long de ce processus de recherche m'a permis d'en arriver à bout. Sa pédagogie et sa méthodologie m'ont été essentielles à l'élaboration de ce mémoire. Ma gratitude va aussi aux professeurs Ismaïl Biskri et François Meunier qui, de par leurs minutieuses corrections, m'ont permis d'améliorer ce mémoire.

Je suis également très reconnaissant envers mes collègues du laboratoire « LAMIA » de l'Université du Québec à Trois-Rivières qui ont collaboré à travers nos différents échanges à la réalisation de ce travail.

Je souhaite également remercier l'ensemble du corps professoral de l'Université du Québec à Trois-Rivières pour leur diligence et leur partage de savoir.

Enfin, mes vifs remerciements vont à ma famille qui durant l'ensemble de mon parcours m'a soutenue, chérie et toujours poussée vers l'avant.

Résumé

Le réseau Véhicule à Grid (V2G) se focalise sur les messages échangés entre le véhicule électrique (PEV) et la borne de rechargement (EVSE). Ces différents messages peuvent impliquer plusieurs types de données dont certaines de nature privée, il est alors nécessaire de sécuriser les différents messages afin de les protéger contre d'éventuels attaques.

La sécurisation du réseau V2G passe par la mise en place d'une infrastructure à clé publique (PKI). Il existe cependant plusieurs types d'architectures PKI pouvant être adaptées aux spécificités du réseau V2G. Nous avons dans un premier temps présenter le V2G et le PKI en général, tout en spécifiant les différents modèles communément utilisés ou « Trust Models » et en discutant du modèle le mieux adapté selon les spécifications du standard ISO 15118.

Ensuite, nous avons utilisé des attaques usuelles sur le réseau afin d'étudier le comportement de notre infrastructure. Nous avons utilisé plusieurs métriques comme le nombre total de paquets perdus, le délai d'authentification et le délai d'envoi de message pour évaluer les performances des diverses propositions afin de renforcer la sécurité des échanges sur les réseaux V2G. Nos solutions améliorent la sécurité du réseau V2G.

Abstract

The Vehicle to Grid (V2G) networks are focused around messages exchanged between the Plug-in Electric Vehicle (PEV) and the Electric Vehicle Supply Equipment (EVSE). These messages can involve many kinds of data including some of private nature, it is then necessary to secure all these messages in order to shield them against possible attacks.

Securing the V2G networks involves setting up a public key infrastructure (PKI). However, there are several types of PKI architectures that can be adapted to the specificities of the V2G network. In this work, we are first presenting the V2G and the PKI in general, while specifying the various commonly used models or "Trust Models" and discussing the model best suited to the specifications of the ISO standard 15118.

Then, we have set up usual attacks on the network in order to study the behavior of our infrastructure. We have used several metrics such as the total number of packets lost, the authentication delay, and the message delay to evaluate the performance of the different proposals in order to reinforce the security of exchanges in V2G networks. Our solutions improve security in V2G networks.

Keywords

Vehicle-to-Grid, Public Key Infrastructure, ISO 15118, Smart Grid, Secure Messages, Elliptic Curves

Table des matières

Table des figures

Liste des tableaux

Nomenclature

API	Application Programming Interface
EV	Electric Vehicle
EVCC	Electric Vehicle Communication Controller
EVSE	Electric Vehicle Supply Equipment
EXI	Efficient XML Interchange
G2V	Grid-To-Vehicle
IDE	Integrated Development Environment
ISO	International Organization for Standardization
MITM	Man In The Middle
PEV	Plug-in Electric Vehicle
PG	Power Grid
PKI	Public Key Infrastructure
SECC	Supply Equipment Communication Controller
SG	Smart Grid
V2G	Vehicle-To-Grid
XML	Extensible Markup Language

Chapitre 1 - Introduction Générale

Les réseaux V2G sont des systèmes basés sur la communication d'un ou plusieurs PEV (« Plug-in Electric Vehicle ») avec une PG (« Power Grid ») dans le but d'échanger de l'énergie. Dans le cas de la présence d'une SG (« Smart Grid »), l'énergie peut être envoyée dans les deux sens, on parle alors de réseau bidirectionnel. Les travaux entrepris sur les réseaux V2G sont assez récents et la plupart des études ont été publiées entre 2010 et nos jours, tandis que les travaux sur les Smart Grid remontent à fin 2007. Comme la demande en électricité se fait de plus en plus importante avec l'accroissement constant de la population, il s'est alors posé la question de la fourniture de cette énergie. Comme présenté dans "Smart Grid: The Electric Energy System of the Future" [**1**], l'idée est d'optimiser la production électrique de manière à réduire les coûts de production en incluant les différents types de productions électriques (éolienne, solaire, hydro-électrique ...) et de réguler intelligemment la demande en éduquant les consommateurs.

Le réseau V2G est quant à lui né de l'opportunité présentée par la multiplication de l'utilisation de véhicules électriques de tout type (hybride, solaire ou exclusivement rechargeable). En effet, ces dernières années, nous avons pu constater l'évolution de la part de marché des véhicules électriques. Nous constatons qu'aux États-Unis, on est passé de 9750 à 71 044 voitures électriques en circulation entre 2011 et 2015 [**2**]. Aussi en prenant le cas du Québec comme exemple, la croissance du parc automobile électrique est de 60.7%, en date du 31 décembre 2016, par rapport à la fin d'année 2015 et cela bien que le marché automobile dans son ensemble recule de 2% [**3**]. Le potentiel proposé par ces véhicules électriques en croissance constante est non négligeable et les experts considèrent ainsi comme important l'apport des PEV, qui pourraient permettre d'adoucir les pics de demande en se rechargeant dans les périodes de basse consommation et en remettant l'énergie dans les périodes hautes. En prévoyant la flambée des prix du carburant avec une offre qui a tendance à baisser au fil du temps, les PEV constituent sans nul doute un enjeu important. L'intérêt principal des PEVs au sein du Smart Grid est l'utilisation de la batterie

couplée à la mobilité de la voiture, ce qui fait des PEVs des banques d'énergies ambulantes susceptibles d'être utilisées.

Lorsque l'on parle de réseau V2G, cela implique qu'il y a de la communication entre les différents acteurs de ce réseau. Cette communication entre les PEVs et la grille électrique par l'intermédiaire de la borne de rechargement est régie par un standard : l'ISO 15118. Ce standard est spécifique au réseau Vehicle-to-Grid, car il détermine les différentes règles utilisées pour l'ensemble des échanges du réseau et cela de manière bidirectionnelle.

Le standard ISO 15118 ne date que de 2013 pour sa première partie et est toujours en cours de développement. Il se compose pour l'instant de trois parties : la définition des cas d'utilisations, la définition des protocoles réseau et de la cinématique des communications et les spécifications physiques telles que le câblage. Le document ISO 15118 représente donc l'outil de référence relatif au réseau V2G.

Une autre spécificité du réseau V2G est qu'il fait transiter plusieurs types de données. Afin d'intégrer au mieux les véhicules électriques au Smart Grid, il est essentiel que des données liées aux véhicules soient échangées et analysées. Ces données peuvent aller d'un simple historique de charge et décharge, à un l'historique des trajets des utilisateurs, en passant par des informations relatives aux contrats d'approvisionnement en énergie ou d'un moyen de paiement. Ces données peuvent être utiles à un algorithme décisionnel permettant de réguler la revente de l'électricité (« carbitrage » [**4**]) ou la priorité de rechargement d'un véhicule. Cependant, on constate que certaines de ces données portent un caractère sensible et leur libre circulation sur le réseau est problématique. Ainsi, comme tout réseau, le V2G a besoin de sécurisation. Le standard ISO 15118 bien qu'abordant différents aspects de la sécurité tels que l'organisation des certificats ou la mise en place du chiffrement ne couvre pas tous les besoins sécuritaires et laisse place à différentes implémentations de ces recommandations.

On peut ainsi distinguer plusieurs approches sécuritaires en rapport au réseau V2G :

1) L'approche standardisée de l'ISO 15118 ;
2) Les propositions issues des recherches indépendantes

Les raisons pour lesquelles il est utile de considérer les différentes recherches citées dans la littérature bien qu'il existe un standard spécifique au V2G sont d'une part que

le standard est toujours en cours de développement laissant ainsi certaines questions sécuritaires en suspens et d'autre part que le standard est lui aussi amener à évoluer et qu'il pourrait bien recevoir des révisions pour donner suite aux apports des travaux de recherches indépendants.

Il est aussi à noter que les recherches citées dans la littérature ont plusieurs manières d'aborder la sécurité parce qu'elles ne traitent pas toutes d'un point de vue global et aussi en partie parce qu'elles ont des objectifs différents, soit d'améliorer l'existant en modifiant certains aspects, soit d'adapter une solution, appliquée dans un autre contexte, au réseau V2G.

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 V2G fait face. Le chapitre 3 permet d'introduire le concept d'infrastructure à clé publique et d'en détailler le fonctionnement ainsi que les différents modèles couramment utilisés. Le chapitre 4 consiste en une revue des travaux réalisés dans le domaine. Dans le chapitre 5 nous proposons notre infrastructure PKI et déterminons les objectifs attendus en termes de sécurité. Nous présentons dans le chapitre 6 l'environnement de simulation utilisé pour nos différents tests et les résultats obtenus au cours de nos simulations. Enfin, le chapitre 7 nous permet de conclure ce travail.

Chapitre 2 – Généralité sur le réseau V2G

2.1 – Introduction

Dans cette partie nous allons présenter de manière sommaire le réseau V2G. Nous allons spécifier les acteurs du réseau ainsi que leur manière d'interagir, ensuite nous allons mettre en relief les implications sécuritaires liées au V2G.

2.1.1 – Les acteurs du V2G

Dans le réseau Vehicle-to-Grid, il existe deux types d'acteurs : les acteurs primaires et les acteurs secondaires.

- Acteurs primaires :

Le véhicule électrique est un acteur primaire (ou principal). Il se compose d'un contrôleur de communication, d'une interface homme-machine, d'une batterie et d'une unité de contrôle électronique.

La borne de recharge est aussi un acteur principal, elle se compose d'un compteur électrique, d'une interface homme-machine, et d'une unité de paiement.

Les deux acteurs principaux communiquent entre eux par le biais de leur contrôleur de communication. Les messages échangés sont alors régis par le protocole ISO 15118.

- Acteurs secondaires :

Les acteurs secondaires sont : l'opérateur de mobilité, le fournisseur électrique et le constructeur automobile.

Les acteurs secondaires n'interviennent pas directement dans les cinématiques d'échanges dans le réseau V2G.

Le tableau 1 permet de résumer le statut de chaque acteur du réseau V2G.

Acteurs principaux	Acteurs secondaires
Véhicule électrique	Opérateur de mobilité
Borne de rechargement	Fournisseur électrique
	Constructeur automobile

Tableau 1: Les acteurs du V2G

Comme les deux principaux acteurs du V2G possèdent un contrôleur de communication à travers lequel ils établissent une correspondance, alors, cette correspondance se fait à travers l'échange de fichier de type EXI. C'est un fichier au format binaire XML, qui permet de réduire la taille et la longueur du traitement des messages [**5**].

2.2 - Les enjeux sécuritaires

2.2.1 – Sensibilité des données

Les renseignements personnels ou privés ne sont généralement pas associés à l'industrie des services publics. Mais en réalité, cette industrie gère des informations clients depuis sa création. La gestion et la livraison d'énergie domestique aux particuliers nécessitent que les compagnies de services publics recueillent certaines informations. La question est de savoir s'il existe ou non des lois pouvant s'appliquer à ces compagnies afin de protéger ces informations. Les données relatives à la vie privée sont définies dans quatre différentes catégories incluant les informations personnelles, les données privées, les données comportementales et les communications privées.

Les informations personnelles sont considérées comme étant les aspects d'un individu, ou des identificateurs spécifiques à cet individu. Il est d'usage lorsque l'on crée un compte auprès d'une compagnie d'électricité ou que l'on contracte auprès de celle-ci pour la fourniture en électricité de son véhicule électrique de fournir à la société de services publics ou privés des informations qui nous sont propres. Le formulaire exige habituellement un nom, une adresse, un numéro de téléphone ou un numéro d'assurance social. Un nom seul ne correspond probablement pas à la définition faite plus haut, cependant, la combinaison du nom et de l'adresse ou de toute autre information citée précédemment répond certainement à l'unicité de cette information. L'acceptation de ces informations par la société de service les qualifie comme informations personnelles, car elle signifie que l'identité d'une personne est correcte. De plus, le numéro d'assurance sociale peut être utilisé pour fournir une authentification que les données fournies représentent bien le demandeur.

Les données privées sont définies comme de l'information qui n'est destinée qu'à l'usage de son propriétaire et dont le partage est limité. L'information recueillie par une société de service public ne répond traditionnellement pas à ce critère, car elle n'en a pas besoin pour offrir un service à l'usager. Ces informations ne représentent donc pas les renseignements qu'un utilitaire souhaite obtenir. Cependant, on peut parfois considérer que les informations relatives au paiement des services font partie du domaine privé, car généralement tenues secrètes par l'usager et considérées comme confidentielles par les sociétés de services.

Les données comportementales représentent les informations personnelles relatives aux activités d'un individu. Elles peuvent aussi bien couvrir les centres d'intérêt de l'individu en général que des données spécifiques telles que son opérateur Internet ou son modèle de téléphone. Ces données sont souvent utilisées pour le ciblage publicitaire.

Alors que les informations associées à une demande de service ne constituent pas à elles seules des données comportementales, si elles sont associées aux informations concernant les données d'utilisation de l'énergie, elles le pourraient. Le résultat est que les entreprises de services publics peuvent être préoccupées par la confidentialité comportementale avec dans un premier temps la mise en place des Smart Grid, et dans un second temps, l'association des Smart Grid aux véhicules électriques.

L'un des aspects des Smart Grid au niveau du consommateur est d'essayer de manipuler le comportement des utilisateurs en leur fournissant des incitations à changer de comportement. Cela peut être illustré par des programmes de tarifications évolutifs en fonction de la demande en électricité (heure creuse, heure pleine), qui permettent d'établir un profil des utilisateurs et de les encourager à changer de comportement en fonction des incitations. Il faut cependant noter que le changement relève entièrement du consommateur. Cependant si une personne mal intentionnée est capable d'avoir accès à cette information, ledit attaquant serait par exemple à même de définir les habitudes d'un usager et de déterminer par exemple quand celui-ci est habituellement absent de son domicile.

Dans le cas du réseau V2G, au niveau du consommateur il est probable que des données comportementales soient utilisées dans des buts similaires à ceux des Smart Grid. Parmi ces données on pourrait retrouver un historique de navigation.

La sécurité des communications personnelles se réfère au droit de communiquer sans surveillance ou censure injustifiées. Pour que ce type d'information constitue un problème dans un réseau Smart Grid ou V2G, les services publics devraient hypothétiquement utiliser les informations qu'ils obtiennent pour surveiller les communications des consommateurs. Cela n'étant aucunement l'objectif des efforts d'implémentation des deux réseaux cités précédemment, il est probable que cela ne représente pas un aspect dont les utilitaires devraient généralement se sentir concernés.

En raison de ces quatre catégories, les services publics ont une préoccupation générale liée à la protection de la vie privée en ce qui concerne les renseignements personnels qu'ils recueillent sciemment et ceux liés au comportement. Tout cela est lié à ce qui pourrait arriver si une menace liée à la sécurité informatique réussissait à subtiliser cette information. En conséquence, les services publics peuvent être tenus de prendre des mesures dans un effort pour empêcher ce vol de données afin de se défendre contre toute responsabilité. C'est principalement parce qu'ils doivent recueillir des informations personnelles afin de fonctionner et devront recueillir des renseignements liés aux habitudes comportementales que la sécurité doit être une composante importante du réseau V2G.

Nos noms, adresses et numéro de téléphone sont requis afin que l'utilitaire puisse nous cataloguer en tant que client et s'assurer que nous résidons sur leur territoire de service. Cette information peut être considérée comme personnelle ou privée, mais il est relativement courant que les consommateurs fournissent cette information. Lorsque l'on obtient un numéro de téléphone par exemple, la compagnie recueille ces informations puis les publie dans un annuaire. Même s'il est possible de demander que ce numéro soit considéré comme privé, les sociétés de services publics ne sont pas dans l'optique de publier ces informations. Néanmoins ils les conservent, et cela est généralement accepté.

Cependant, les numéros d'assurance sociale sont parfois également requis et utilisés pour effectuer une vérification des antécédents financiers afin de déterminer la capacité du demandeur à effectuer des paiements mensuels suite à un contrat de fourniture électrique automobile.

2.3 – Conclusion

Dans cette section, nous avons introduit le réseau V2G en présentant les différents acteurs qui interagissent dans le réseau, ainsi que leur moyen de communiquer. Ensuite, nous avons introduit les différents enjeux sécuritaires relatifs au V2G, notamment le besoin de sécurisation des données du réseau qui se révèlent parfois être particulièrement sensibles.

Dans le chapitre suivant, nous aborderons les infrastructures à clés publiques (PKI). L'introduction des PKI est une étape importante car elle nous permet de comprendre comment ces dernières nous sont utiles à l'atteinte de nos objectifs sécuritaires.

Chapitre 3 – Généralités sur les infrastructures à clé publique

3.1 – Introduction

L'Internet Engineering Task Force (IETF) définit le PKI (Infrastructure à clés publiques) comme étant la mise en commun d'un ensemble de ressources, matérielles et humaines, alliée à la mise en place de règles régissant l'utilisation de certificats issus de la cryptographie asymétrique. Ceci dit, l'infrastructure de gestions des clés permet d'effectuer des échanges sécurisés.

Elle procure des certificats attestant de la relation existante entre une clé publique et son détenteur. Elle s'occupe de la gestion des paires de clés asymétriques dans un climat de confiance et assure lors des échanges entre des parties, les principaux points suivants :

- Protéger les données et les identités de toute fuite éventuelle ;
- Assurer l'identification de l'utilisateur ;
- Procéder à une vérification des entités présentes lors des échanges ;
- Protéger les données de toute modification ou altération.

La PKI assure cette sécurité à travers un ensemble de services parmi lesquels nous citons :

- L'enregistrement des ressources (humaines ou informatisées) ;
- La gestion des certificats, la liste de révocation et les utilisateurs

Ces services seront détaillés dans la suite de ce document.

3.2 – Les composants de l'infrastructure

L'infrastructure de gestion des clés est basée sur plusieurs composants qui sont indispensables à son fonctionnement. Parmi ces composants, nous répertorions comme principaux, les suivants.

3.2.1 – L'autorité de certification (CA)

On peut dire que c'est le composant le plus important de l'infrastructure PKI du fait de son rôle central dans les différentes cinématiques d'échanges à l'intérieur d'une PKI.

La CA est chargée de délivrer et gérer les certificats. En effet, elle génère des certificats à clés publiques et assure l'intégrité et l'authenticité des informations contenues en les signant avec sa clé privée. Pour émettre des certificats, elle doit recevoir, au préalable, les requêtes de certification contenant la clé publique de l'entité qui le sollicite.

3.2.2 – L'autorité d'enregistrement (RA)

Elle joue le rôle d'intermédiaire entre l'utilisateur et la CA et dépend de cette dernière. Elle a comme responsabilité de vérifier tout ce qui concerne l'utilisateur, son identité, la concordance entre clés privées/publiques, de certifier et d'assurer qu'il possède les droits nécessaires pour demander des certificats. En résumé, cette autorité a pour tâche de gérer les requêtes de certificat qu'elle reçoit des différentes entités et de concevoir les paires de clés qui leur sont spécifiques.

3.2.3 – Les certificats

Ils assurent la sécurité d'une clé publique afin d'éviter les failles de sécurité liées à l'usurpation d'identité et à la modification écrite. Leur rôle dans le fonctionnement des PKI sera abordé plus en profondeur dans la suite du document.

3.2.4 – Les services d'archivage et de publication

L'archivage est un service qui permet le stockage des paires de clés pour une restitution en cas de perte de la clé privée. En effet, il a pour mission de stocker en toute sécurité les clés de chiffrement émis au sein de l'infrastructure.

La publication est un service qui répertorie les différents certificats à clés publiques émis par la CA afin de les rendre disponibles aux éventuels futurs utilisateurs, c'est pourquoi on se réfère communément à lui par le terme de dépôt. Ainsi, un annuaire peut être utilisé (LDAP ou X500 par exemple), un serveur Web ou encore un outil de messagerie, etc.

Ce service est contraint par plusieurs exigences telles que, par exemple, le délai de mise à jour des listes de révocation ou la disponibilité de ces listes. Le dépôt est également responsable de la publication de la CRL (Liste de Révocation de Certificat).

3.2.5 – Les utilisateurs

Ce sont les personnes ou entités organisationnelles ayant émis ou émettant des demandes de certificat, ou souhaitant simplement vérifier la validité et les informations sur l'identité d'un certificat préalablement reçu.

En plus des principaux composants que nous venons de voir, nous avons aussi quelques-uns dits complémentaires, à savoir : les bases de données, le serveur d'horodatage, les serveurs HTTP, SMTP, POP.

3.3 – Principe de fonctionnement des infrastructures de gestion de clés publiques (PKI)

Le principe de fonctionnement des infrastructures de gestion de clés repose essentiellement sur les services précédemment cités.

Les services que l'infrastructure PKI fournit doivent obligatoirement être précédés d'une mise en place d'une entité capable d'effectuer la gestion des différents certificats. Ces services se basent sur des composants tels que nous avons vu préalablement.

Ainsi le fonctionnement d'une PKI se compose de plusieurs étapes :

1. Générer les clés, qui se fait aléatoirement de sorte à garantir leur non-prédictibilité ;
2. Enregistrer les clés, permettant de garder toute leur intégrité et cela de manière confidentielle ;
3. Générer les certificats ;
4. Révoquer un certificat, en cas de corruption de ce dernier. Une fois révoqué celui-ci est consigné dans une CRL (Liste de Révocation de Certificat) ;
5. Supprimer une clé, lorsque celle-ci est expirée ou pose un problème de sécurité.
6. Archiver une clé, afin de garder une trace de celle-ci même après une mise au rencart, afin d'assurer la continuité du travail achevé avec cette dernière.

Nous noterons aussi que de nombreuses applications profitent de la sécurité fournie à travers l'utilisation des infrastructures à clés publiques. Parmi elles, nous avons retenu :

- L'accès à Internet

  À travers les navigateurs et serveurs Web qui utilisent le chiffrement pour l'authentification et la confidentialité, mais surtout au niveau du e-commerce qui incite à des transactions financières : ceci implique l'utilisation de protocoles tels que SSL (Secure Sockets Layer), qui permet d'effectuer des échanges sécurisés sur Internet.

- La messagerie

  Afin de sécuriser la messagerie, l'utilisation des paires de clés est nécessaire pour la sécurisation des messages, fichiers et signatures. Le protocole utilisé est le S/MIME (Secure Multipurpose Internet Mail Extensions), ce protocole gére la confidentialité des courriels.

- Le réseau privé virtuel

  Le chiffrement des données et l'authentification sont les deux principales fonctions utilisées pour gérer les liens entre les différentes parties au sein d'un réseau privé virtuel (Virtual Private Network (VPN)). Afin d'assurer la confidentialité entre les paires ou équipements (site-to-site, router-to-router) et pour sécuriser les connexions à distance (client-To serveur). Cependant, l'IETF a intégré ces services dans le protocole IPSec afin de la sécuriser les tunnels VPN.

Le fonctionnement des infrastructures à clé publique repose fondamentalement sur les mécanismes de gestion des certificats et de signature numérique.

Un certificat numérique est un document électronique permettant l'association entre une clé publique et une entité (personne, équipement (dans le cas du réseau V2G), entreprise...) afin d'assurer sa validité. On peut donc établir de façon triviale que le certificat est le lien entre une entité physique et une entité numérique, certifié par le CA.

Il existe plusieurs types de certificats qui sont présentés en différentes classes selon le niveau de sécurité :

- Classe 1 : Requiert une adresse courriel du demandeur ;
- Classe 2 : Exige une preuve d'identité du demandeur (document d'identification, numéro de série unique, etc.) ;
- Classe 3 : Exige la présence physique du demandeur.

Comme présenté dans la figure 1, les certificats ont un cycle de vie composé des phases suivantes :

1. Demande de certification ;
2. Vérification des attributs ;
3. Création et signature du certificat ;
4. Remise au demandeur (publication) ;
5. Utilisation du certificat ;
6. Suspension ou révocation du certificat ;
7. Expiration du certificat (possible renouvellement).

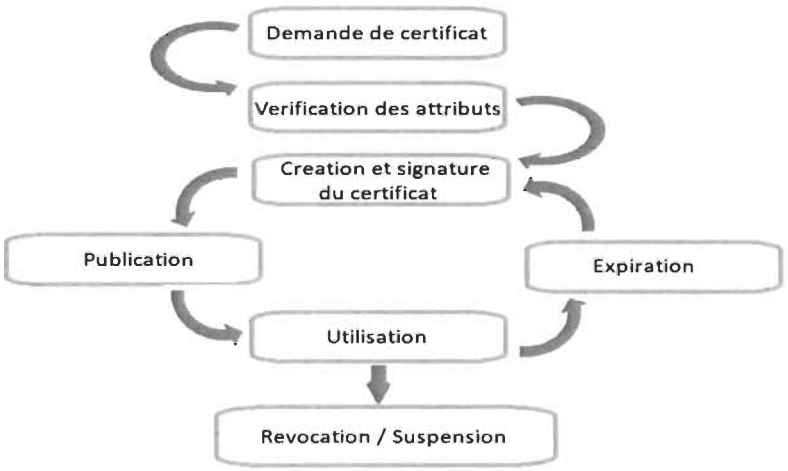

Figure 1: Cycle de vie d'un certificat

Le standard régissant les certificats numériques est le X.509. Il s'agit d'une norme cryptographique soumise par l'UIT (Union Internationale des Télécommunications) mise en place dans les PKI notamment. La norme X.509 définit un certificat en plusieurs champs :

- Numéro de version : identifie la version du X.509 ;
- Numéro de série du certificat : propre au CA ;
- Identifiant de l'algorithme du certificat : algorithme utilisé pour la signature ;

- Émetteur : « Distinguished Name » (DN) du CA émettant le certificat ;
- Période de validité : intervalle de temps représentant la durée de vie du certificat ;
- Demandeur : DN du détenteur de la clé publique ;
- Information de la clé publique du demandeur : nom de l'algorithme à clé publique, paramètres concernant la clé.

Les certificats émis le sont pour une durée déterminée et suivent le cycle de vie abordé précédemment. Les certificats peuvent être suspendus à la demande du détenteur ou pour des raisons de sécurité.

La signature numérique est définie comme « un mécanisme permettant de garantir l'intégrité d'un document et d'en authentifier l'auteur ». Ainsi, une signature électronique ne peut être falsifiée, réutilisée dans un autre document, reniée, ni altérée.

Lorsque l'on parle de signer numériquement un document, il s'agit alors d'effectuer un chiffrement du dit document à l'aide de sa clé privée, qui est connue uniquement du propriétaire légitime. La signature est infalsifiable, car c'est la clé privée qui l'a générée au moment de la signature. La signature assure, par ailleurs, l'intégrité du document du fait que toute altération serait automatiquement décelée lors du déchiffrement. Il est tout de même préférable d'effectuer la signature sur le hash du message, obtenu à travers une fonction de hachage, à envoyer afin de réduire le temps d'exécution de l'opération tout en garantissant l'authenticité de celui-ci, étant donné les chances infinitésimales d'obtenir un même hash à partir de deux messages différents. Ainsi à la réception du document, il est possible d'identifier l'entité émettrice à l'aide de sa clé publique, et de s'assurer de la non-altération du message grâce à l'empreinte de celui-ci.

Une fonction de hachage aussi appelée fonction de condensation est une fonction permettant d'obtenir un condensat (ou empreinte) d'un texte, c'est-à-dire une suite de caractères relativement courte spécifique au message (ou document) condensé. Il s'agit d'une fonction mathématique à sens unique qui permet de calculer à partir d'une suite binaire une chaîne de caractères qui fera office d'empreinte numérique. Ainsi lorsque la suite binaire est altérée, l'empreinte l'est aussi. Les fonctions de hash les plus utilisées sont :

- MD5 (Message Digest), créant une empreinte d'une taille de 128 bits
- SHA (Secure Hash Algorithm), créant des empreintes à partir de 160 bits

3.4 – Les modèles et les architectures PKI

Les relations entre les composants de l'infrastructure à clé publique sont catégorisées en modèle et architecture selon la situation dans laquelle l'infrastructure PKI est mise en place.

Chaque autorité de certification à un nombre d'entités avec lesquelles elle communique, qui permet le contrôle plus ou moins aisé des échanges.

3.4.1 – Les modèles

Les modèles les plus couramment utilisés sont appelés « Trust Models » ou modèles de confiance, car ils ont été maintes fois éprouvés. Les « Trust Models » sont les suivants :

- Certificate Trust List (CTL)

  Le modèle de confiance basé sur la liste des certificats de confiance demande dans un premier temps que l'utilisateur envoie sa clé publique à l'autorité de certification (CA) via un canal sécurisé. Après réception, l'autorité de certification envoie à l'utilisateur sa clé publique en plus d'un certificat qu'elle a signé avec sa clé privée. L'autorité de certification envoie ensuite sa clé publique au gestionnaire de liste de confiance (GLC), puis le GLC envoie sa propre clé au système de vérification et tout cela se fait sur un canal de transmission sécurisé.

  Entre temps, le GLC utilise une fonction de hachage pour créer une empreinte de la clé publique du CA et l'envoie au système de vérification qui dès lors dispose de tous les éléments pour vérifier l'identité des interlocuteurs (CA, GLC, utilisateur). Aussi, l'utilisateur peut effectuer tout envoi de données et il suffira alors qu'il signe et joigne le certificat du CA à son message.

- Certificate Request Message

  Le fonctionnement de ce modèle est presque similaire au précédent : en premier lieu, l'utilisateur envoie sa clé publique vers une autorité, cette fois-ci, l'autorité

d'enregistrement des certificats (RA), mais toujours à travers une liaison sécurisée.

La RA transfère un message signé au CA ; ce message inclut, en plus des informations concernant l'utilisateur, la clé publique de l'utilisateur : c'est ainsi qu'est émise la demande de certificat. L'utilisateur recevra alors de la part de l'autorité de certification, un certificat signé.

Enfin, après que le CA ait envoyé sa clé publique au système de vérification, l'utilisateur pourra transmettre les données qu'il devra signer et accompagner du certificat qui lui a été délivré afin que le système de vérification puisse confirmer leur authenticité.

- Out of Band Mechanism (OOB)

C'est un modèle de confiance qui permet de créer une empreinte de la clé d'une CA de manière sécurisée (à l'aide d'une fonction de hachage). Une fois créée, la clé peut être acheminée sur un réseau peu, voir non sécurisé.

Le destinataire à qui on a au préalable fourni les informations concernant la fonction avec laquelle cette empreinte a été générée pourra comparer à la réception et vérifier si les données n'ont pas été altérées afin de pouvoir en récupérer de manière sûre la clé de la CA.

Cette technique est communément utilisée pour sécuriser les protocoles sur les navigateurs et serveurs Web.

- Cross Certification

Le modèle de certification croisée propose une architecture à deux CA. Elle est plus sécurisée et permet d'avoir les traces de toutes les transactions effectuées.

L'utilisateur envoie sa clé publique à une première autorité de certification qui lui renvoie un certificat signé avec sa clé privée. Via des liaisons sécurisées, la clé publique du CA1 est transmise au CA2 et celle du CA2 est envoyée au système de vérification. Le CA2 établit et envoie au système de vérification un certificat croisé, c'est-à-dire la clé publique de la première autorité signée de la clé privée de la seconde autorité. Enfin, l'utilisateur peut envoyer des données qu'il aura préalablement signées et accompagnées du certificat qui lui a été fourni. Le

système de vérification se charge désormais de la sécurité lors de l'échange des données.

3.4.2 – Les architectures

L'infrastructure PKI est généralement composée de plusieurs CA reliés par des « trust paths » ou chemins de confiance. Selon l'environnement, les CAs peuvent être organisés de manière complètement différente et de leur architecture dépendra l'adaptabilité du modèle de confiance. Ainsi, les architectures les plus couramment utilisées sont les suivantes :

- L'architecture hiérarchique

Le fonctionnement de cette architecture dans le cas de deux autorités de certification (CA1 et CA2) régies par une autorité de certification centrale ou « CAroot » est le suivant : CA1 et CA2 envoient leur clé publique au CA central qui génère un certificat pour chacun des deux CA. Au sein de cette architecture, le « CAroot » a le plus haut niveau d'autorité et possède donc un certificat autosigné. Aussi, cela implique que tous les composants de l'architecture placent leur confiance dans le CA central.

- L'architecture P2P (Peer-to-Peer)

En opposition à l'architecture hiérarchique, l'architecture Peer-to-Peer place les différents CA au même niveau d'autorité. On arrive alors à une situation dans laquelle les certificats sont cosignés, le CA1 pouvant signer des certificats pour le CA2 et vice-versa. L'inconvénient de cette architecture est alors le besoin d'échange mutuel des différentes clés publiques pour qu'un CA génère des certificats pour ses homologues.

- L'architecture en pont

L'architecture en pont ou « Bridge » est une association des deux architectures précédemment abordées. Comme l'architecture hiérarchique a pour principales lacunes la disponibilité et la sécurité et que le modèle pair-à-pair est ralentit par la multitude d'échanges qui y sont générés, alors l'architecture en pont palie aux lacunes des deux architectures précédentes.

Son fonctionnement est similaire à celui du P2P à la différence que les échanges entre CA qui ralentissaient le P2P sont réduits dans la mesure où les CAs n'échangent leurs clés qu'avec l'autorité pont. On peut aussi définir cette architecture comme une architecture hiérarchique où le CAroot est au même niveau d'autorité que les autres CAs qui y sont affiliés.

La figure 2 et le tableau 2 présentent une comparaison des trois architectures citées ci-haut.

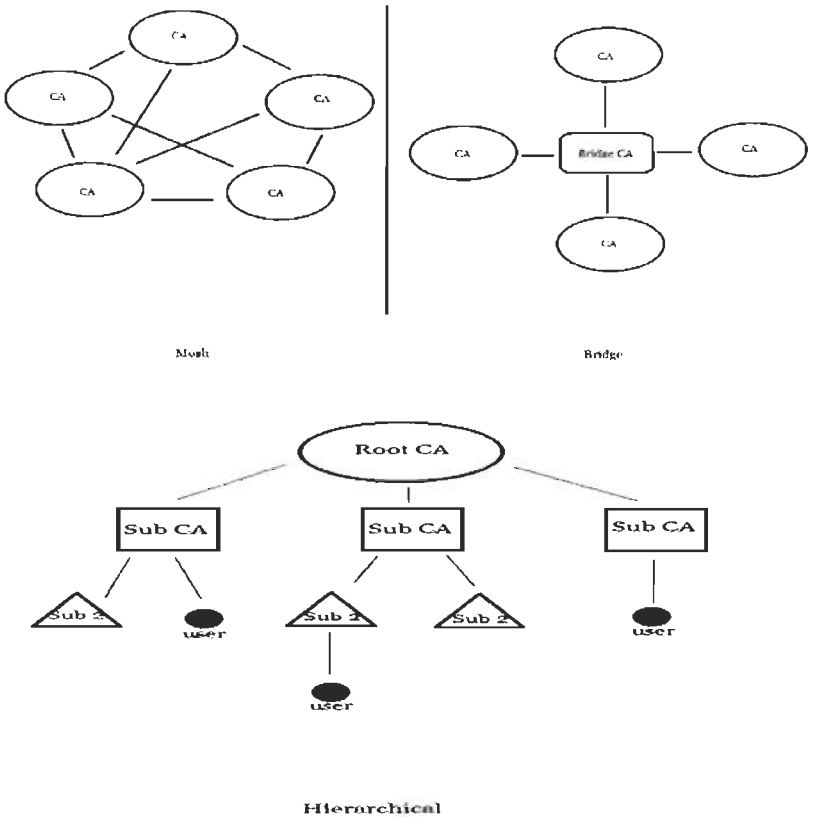

Figure 2: Les architectures PKI

Type d'architecture	Avantages	Inconvénients
Classique (Hiérarchique)	• Adapté à une grande implémentation	• Non flexible • Problème en cas d'indisponibilité du Root CA
Mesh	• Flexibilité	• Non adapté à une grande implémentation • Difficulté à remonter une chaîne de confiance
Bridge	• Interopérabilité entre	• Problème en cas

	PKI • Flexibilité • Adapté à une grande implémentation	d'indisponibilité du Bridge CA

Tableau 2: Comparaison des architectures PKI

3.5 – Conclusion

Dans ce chapitre, nous avons présenté de manière détaillée les infrastructures à clés publique. L'utilisation d'une infrastructure PKI sera le point central de notre proposition pour sécuriser les réseaux V2G (chapitre 5). Dans le chapitre suivant, nous présenterons l'état de l'art sur la sécurité des réseaux V2G en discutant les points forts et les points faibles de chaque proposition.

Chapitre 4 – Revue de littérature

4.1 – Introduction

Les travaux et les réflexions sur l'utilité d'une grille électrique intelligente afin de remplacer l'implémentation actuelle datent de quelques années maintenant et ce n'est que récemment que les recherches sur la sécurisation de cette grille ont commencé à se développer. Bien que les enjeux sécuritaires des Smart Grid ne soient pas exactement les mêmes que ceux du V2G, ils partagent tout de même plusieurs similarités, de par les données qui y transitent et de leur structure hiérarchisée. Comme expliqué par H.Gharavi et R.Ghafurian, le réseau V2G est partie intégrante de l'évolution naturelle dans laquelle s'est lancée la grille électrique classique [1]. Afin de protéger les différentes données transitant sur le réseau, plusieurs travaux ont été entrepris.

Dans ce chapitre, nous allons tout d'abord introduire le standard ISO 15118 qui régit les échanges au sein du réseau V2G. Ensuite, nous abordons les différents travaux pertinents associés à la sécurisation des Smart Grid en général et du réseau V2G en particulier. Enfin, nous présenterons les différentes solutions cryptographiques employées.

4.2 – Le standard ISO 15118

Le standard ISO 15118 est spécifique au réseau V2G, car il détermine les différentes règles utilisées pour tous les échanges entre un véhicule électrique (EV) et une borne de rechargement (EVSE) et cela de manière bidirectionnelle [**6**].

Le standard ISO 15118 se divise en trois différentes parties :

- 15118-1 : Définit les cas d'utilisation du standard ISO 15118
- 15118-2 : Se rapporte aux couches 7 à 3 du modèle OSI (protocoles réseau, initiation de communication ...)
- 15118-3 : Se rapporte aux couches 1 et 2 du modèle OSI (câblage et autres spécifications physiques)

Cependant, le standard ISO 15118, bien qu'abordant différents aspects de la sécurité tels que l'organisation des certificats et la mise en place du chiffrement, ne spécifie pas l'architecture PKI exacte qui sera employée.

4.2.1 – Les certificats

L'ISO 15118 émet plusieurs recommandations quant à la gestion des certificats, ces recommandations sont les suivantes :

- Tous les acteurs du réseau V2G doivent supporter les certificats X.509-3 (cf. Standard X.509).
- Les validations de certificats doivent être effectuées en accord avec le standard RFC 5280.
- Un certificat n'est considéré comme valide que si le certificat racine est considéré comme conforme.
- La vérification de la période de validité des certificats doit être supportée par le périphérique de communication du véhicule (EVCC).
- Le certificat utilisé par le périphérique de communication de la borne (SECC) doit toujours être valide.
- Chaque EVCC doit supporter au moins un certificat racine.
- Chaque SECC doit supporter le stockage d'au moins 10 certificats racines.
- La longueur du chemin de confiance d'un certificat de doit pas excéder 3 (deux CA intermédiaires avec le CAroot).
- Les certificats doivent être encodés sous le format DER (Distinguished Encoding Rules) et leur taille ne doit pas excéder 800 bytes.
- La période de validité d'un certificat racine doit être de 40 ans et valide pour les 35 années suivantes.
- Un CAroot ne doit pas disposer de plus de 10 certificats racines valides.
- Un CAroot ne peut délivrer que des certificats autosignés.

Le standard ISO 15118 permet à plusieurs acteurs du réseau V2G d'émettre ou de posséder des certificats, ces différents acteurs sont :

- Autorité de certification racine (CAroot) : Possède le plus haut niveau d'autorité, délivre des certificats permettant de vérifier l'authenticité des

autres certificats du réseau. Les clés privées correspondantes aux certificats racines restent en possession du CA.

- Opérateur de mobilité (MO) : Délivre des certificats permettant de signer les contrats.
- Contrat : Le contrat est ici considéré comme une « entité » dans la mesure où il se voit attribuer un certificat. Ce certificat représente donc le contrat entre le véhicule électrique (EV) et l'opérateur de mobilité et il est stocké, ainsi que la clé privée correspondante, dans le contrôleur de communication du véhicule électrique (EVCC).
- Le contrôleur de communication de la borne (SECC) : Possède un certificat permettant d'authentifier le SECC auprès de l'EVCC. Ce certificat est stocké au niveau du SECC, ainsi que la clé privée correspondante, et est dérivé d'un certificat racine.
- Le constructeur ou « Original Equipment Manufacturer » (OEM) : Il émet deux types de certificats ; les certificats d'approvisionnement qui sont spécifiques à chaque véhicule et permettent de vérifier l'identité du véhicule, et les certificats racines qui permettent de signer les certificats d'approvisionnement.

On obtient alors une architecture globale telle que présentée dans la figure 3.

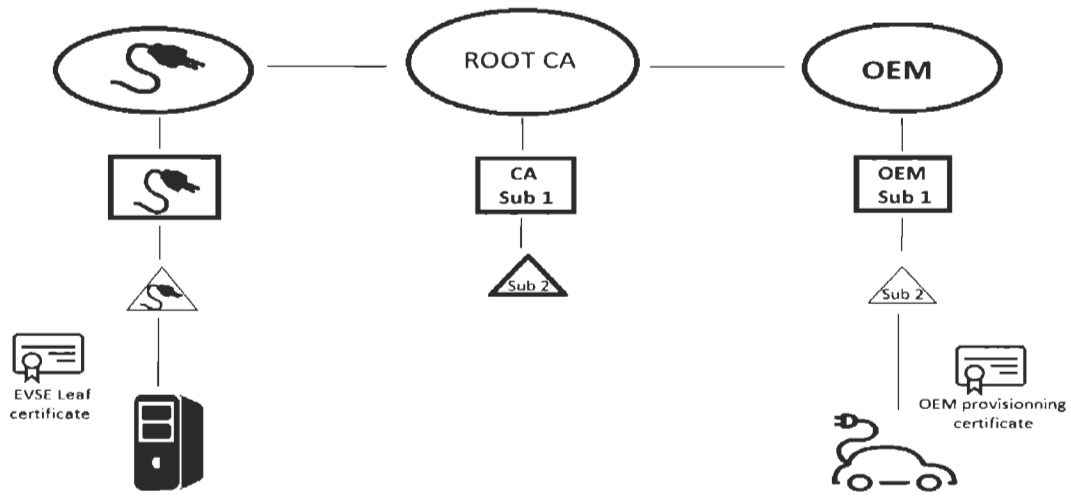

Figure 3: Schéma de la proposition PKI de l'ISO 15118

On constate ainsi que les certificats dérivés des certificats racines du MO et de l'OEM ne sont pas obligatoirement signés par le CAroot. De ce fait, ils ne sont pas à considérer dans l'architecture PKI globale. On peut déduire alors que l'architecture PKI privilégiée par le standard ISO est la structure hiérarchique.

4.2.2 – Les contraintes de l'ISO 15118

Parmi les différentes recommandations énoncées dans le standard ISO 15118, certaines ont été influencées par des contraintes liées aux constructeurs. En effet l'espace nécessaire au stockage dans les véhicules électriques est limité par le coût du stockage, d'où la nécessité de limiter le nombre de certificats stockés dans les EVs ainsi que leur taille.

De plus le nombre de certificats racine obligatoires au niveau de l'EVCC est de seulement un, ce qui pourrait être possible dans un contexte régional, mais qui n'est pas applicable, ou difficilement, à l'échelle mondiale. En plaçant un CAroot à l'échelle mondiale, on devra placer des autorités de certifications secondaires (Sub-CA) au niveau continental, puis au niveau national. La charge supportée par les Sub-CA serait alors très élevée.

En outre, la longueur de la chaîne de confiance est limitée à 3, ce qui implique qu'il y a au maximum deux degrés d'autorités de certifications secondaires (Sub-CA). Dans le cadre d'une implémentation au Canada cela implique par exemple qu'il y ait un CAroot au niveau national, un Sub-CA au niveau provincial et un dernier au niveau régional. Cependant, ISO 15118 préconise de placer le RootCa au niveau continental et prévoit au moins 5 RootCA pour l'ensemble des continents.

Enfin, le réseau V2G une fois implémenté nécessitera une forte disponibilité des différents services de par leurs nécessités, mais aussi de la charge du réseau vu le nombre important et en constante croissance que représentent les véhicules électriques.

Il semble alors que l'architecture en pont est à préconiser dans le cadre de l'ISO 15118 d'une part pour le problème de disponibilité, mais aussi, car l'utilisation d'une autorité pont entre les différents RootCAs pourrait permettre une intégration

nationale des RootCAs plutôt que continental tout en gardant la même longueur de chemin de confiance.

4.3 – Les travaux connexes

4.3.1 – La sécurité au sein des Smart Grid

Afin de mieux comprendre les enjeux sécuritaires du V2G, nous nous sommes penchés sur les différents travaux effectués dans le Smart Grid en nous focalisant sur les aspects que ce dernier pourrait partager avec le réseau V2G. Ainsi nous avons eu à analyser plusieurs travaux de référence.

Tout d'abord, les travaux de Gilbert N. Sorebo et Michael C. Echols dans [7] nous ont permis d'obtenir une vue d'ensemble des Smart Grid, du motif de la création à la sécurisation en passant par le fonctionnement détaillé.

Olivier Kosut, Liyan Jia, Robert J. Thomas et Lang Tang présentent dans [**8**] une recherche qui traite des attaques sur le réseau Smart Grid permettant à un potentiel attaquant de mettre à mal la surveillance du réseau et fausser l'état actuel du réseau. Ce document se focalise sur les erreurs d'estimation dans le monitoring réseau induit par deux différents types d'attaques : « strong attack regime » dans lequel l'attaquant peut prendre le contrôle d'une multitude d'appareils servant à monitorer le réseau ; « weak attack regime » dans lequel les ressources de l'attaquant sont limitées. Dans le premier cas, les auteurs proposent une estimation, du nombre minimal de « smart meters » nécessaire pour fausser l'état du réseau, à l'aide de la théorie des graphes. Dans le second cas de figure, les auteurs proposent l'utilisation de la théorie décisionnelle du point de vue du centre de contrôle (attaqué) et du point de vue de l'individu malintentionné (attaquant).

Similairement, Yao Liu, Peng Nang et Michael K Reiter abordent dans [**9**] des attaques par injection de données. Les hypothèses formulées dans cet article sont similaires à celles de l'article précédent, dans le sens où les auteurs considèrent deux types d'attaques, une où l'attaquant possède les moyens d'accéder à un certain nombre de « meter » (périphériques de mesures) et l'autre où l'attaquant est limité dans ses ressources. Cette fois-ci les auteurs utilisent un modèle de régression

linéaire ($z = Hx + e$, où $\boldsymbol{H}$ est une matrice de dimensions m soit le nombre de meter, $\boldsymbol{x}$ est le nombre de variables d'état et $\boldsymbol{e}$ représente les erreurs de mesures).

Les deux articles [8,9] précédant permettent de mettre en lumière les risques liés à la non-sécurisation des données du réseau dans le cadre du monitoring, ainsi que leurs impacts.

4.3.2 – Les propositions d'infrastructures à clé publique

Sachant que le réseau V2G est une extension du Smart Grid, l'analyse des articles [8,9] du point précédant nous permet de comprendre l'importance de la sécurisation du réseau V2G. Nous avons ainsi tenu à analyser les différents moyens de sécurisation possiblement implémentable dans le V2G.

Dans un premier temps nous avons analysé les travaux de Tim Moses dans [**10**], qui propose une analyse des différents modèles de confiance rencontrés dans le PKI, et de Radia Perlman dans [**11**] qui nous permettent ainsi d'avoir une vision globale des différentes solutions permettant de sécuriser le réseau.

Ensuite, les recherches que Daojing et al. proposent dans [**12**] se focalisent sur la sécurisation des différents réseaux sans fil présent dans une architecture Smart Grid. Les auteurs se livrent donc à un ciblage des caractéristiques nécessaires à la sécurisation des réseaux sans fil du Smart Grid, et expliquent comment les PKI peuvent jouer un rôle important. Cependant, l'auteur met en relief les lacunes des PKI actuelles dans leur usage avec les Smart Grid. En effet, se posent toujours les questions de la disponibilité, de l'adaptabilité et de la protection des éléments privés. La disponibilité peut être mise à mal à travers des attaques de déni de services consistant à envoyer plusieurs faux certificats et signatures à une entité afin d'en occuper les ressources et empêcher les autres entités de s'y connecter. Il est donc nécessaire de remédier à ce problème pour une implémentation efficace des PKI. L'adaptabilité est remise en cause par le fait que le Smart Grid utilise plusieurs types de périphériques. Si ceux déployés dans les Smart Grid supportent les opérations sécuritaires, certains équipements ne sont pas adaptés à une utilisation conjointe à la mise en place d'une infrastructure PKI. La protection des éléments privés implique que chaque entité doit renouveler fréquemment son certificat anonyme, multipliant ainsi le nombre d'entrées dans la liste des certificats. Cette solution est peu

envisageable dans la mesure où certains appareils ne possèdent pas la mémoire nécessaire au stockage d'une liste étendue.

Les travaux de Todd Baumeister dans [**13**] et de Mingchu et al. dans [**14**] se rejoignent dans le sens ou ces derniers abordent les avantages de la mise en place d'une architecture PKI en pont. Dans [**14**], les auteurs visent principalement l'interopérabilité de plusieurs architectures PKI via la mise en place d'un CA en pont, tandis que Baumeister [**13**] propose la mise en place d'une architecture en pont suite à l'analyse des besoins sécuritaires du Smart Grid.

4.3.3 – La protection des données sensibles

Parmi les articles issus de la littérature, deux travaux visant à fournir des mécanismes de protection des données privées nous ont particulièrement servis. Les travaux effectués dans [**15**] proposent la mise en place de mécanismes tels que la signature de groupe pour masquer l'identité d'un émetteur aux entités externes au groupe, le partage de secret afin de subdiviser une donnée en plusieurs parties détenues par des entités différentes. Tandis que, Neetesh Saxena, Bong Jun Choi et Shinyoung Cho proposent dans [**16**] de mettre en place un processus d'authentification propre au V2G limitant les données envoyées sur le réseau et protégeant leur intégrité à travers l'usage de fonction de hash.

4.3.4 – Les solutions cryptographiques

Outre le choix de l'architecture PKI, la sécurisation passe aussi par le choix des procédures de chiffrement.

Les travaux de Liping Zhang, Shanyu Tang et He Luo dans [**17**] suggèrent un protocole d'authentification basé sur les courbes elliptiques dans le Smart Grid. Leur proposition consiste à réaliser une authentification mutuelle entre les acteurs du réseau ainsi que la transmission des identités, en cas de nécessité, de manière chiffrée sur le réseau afin de les rendre inexploitables par un attaquant.

Dans le cas de l'article [**18**], Binad Vaidya, Dimitrios Makrakis et Hussein Mouftah proposent l'utilisation de la cryptographie elliptique pour pallier les limitations actuelles du X.509. Leur solution se repose aussi sur l'utilisation de clé publique autosignée (combinant la clé publique et le certificat). Ces derniers comparent alors

leur solution à l'existant en comparant les tailles de certificats ainsi que les temps de validation.

4.4 – Conclusion

L'analyse des différents modèles PKI nous a amenés à identifier l'intérêt de chacune des architectures PKI ainsi que ses inconvénients. D'autre part, l'analyse des spécifications de l'ISO 15118 nous a permis de mettre en exergue les exigences de ce standard, mais aussi de voir les contraintes liées à son implémentation. Ces deux analyses nous ont ainsi permis d'identifier parmi les modèles de confiance, celui qui est le mieux adapté au standard de régulation du réseau V2G. De plus, l'étude des différents travaux exposés précédemment nous a permis d'obtenir une vision plus élargie de l'impact sécuritaire amener par l'utilisation des PKI ainsi que plusieurs pistes de recherche pour sa mise en place efficiente au sein du réseau. La limite principale des différents travaux exposés dans cette partie, a l'exception du [**18**], vient du fait qu'ils ne proposent pas de données issues de la simulation du réseau dans des conditions proches du réel ou ne traitent pas directement les différentes attaques que pourrait rencontrer le réseau V2G.

Dans le chapitre suivant, nous présentons donc le modèle de sécurité que nous proposons afin de combler au mieux les lacunes exposées dans cette section. Nous détaillons donc les points sécuritaires sur lesquels nous nous sommes focalisés. Ensuite, nous décrivons notre implémentation PKI. Enfin, nous introduisons le simulateur que nous avons utilisé, ainsi que les modifications que nous y avons apportées.

Chapitre 5 – Modèle de sécurité proposé

5.1 – Introduction

L'analyse des différentes architectures PKI évoquées dans le chapitre précèdent nous a permis d'effectuer une proposition d'architecture permettant de garantir plusieurs points sécuritaires essentiels au réseau V2G. Nous allons donc spécifier les différents points sur lesquels s'est focalisée notre approche, ensuite nous détaillerons les caractéristiques de notre implémentation.

5.2 – Points sécuritaires

Les propositions que nous formulons dans notre travail de recherche visent à garantir la préservation des différents points sécuritaires suivants :

- Disponibilité

Les mécanismes de sécurité ne doivent pas empêcher la recharge des véhicules. En effet, l'indisponibilité de la recharge pourrait entraîner une immobilisation des usagers.

- Authentification

L'infrastructure à clé publique doit permettre d'assurer l'identité d'un élément du réseau Vehicle-to-Grid, et ainsi empêcher l'usurpation d'identité. Par exemple, le cas où un véhicule se ferait passer pour un autre lors d'une recharge afin d'éviter de supporter les coûts du service.

- Confidentialité

L'utilisation d'une PKI doit aussi permettre de protéger les données sensibles propres aux différents usagers. Ces données doivent donc être chiffrées tout au long de leur utilisation. Par exemple dans le cadre du V2G, deux types de moyens de paiement ont été prévus, l'une par contrat, et l'autre par un moyen de paiement externe (ex. : carte de crédit). Dans le second cas, les données de paiement doivent être protégées.

- Anonymat

La mise en place du PKI doit assurer l'anonymat des différentes entités. Permettant ainsi de cacher le lien entre les données transmises et leur propriétaire. Dans le cas d'une attaque, cela pourrait permettre de rendre inutilisables les données interceptées par un éventuel attaquant.

5.3 – Méthodologie de recherche

Notre analyse du document de référence de l'ISO 15118 dans le chapitre 4, nous a permis de mettre en lumière un des manques de l'implémentation proposée par le standard. En effet, à cause de la limitation dans la longueur de la chaine de confiance du certificat, il est difficile d'assurer l'interopérabilité du réseau à l'échelle mondiale, ce qui impacte alors la disponibilité.

Nous avons alors recherché dans la littérature des exemples d'implémentations d'infrastructures à clé publiques, permettant de garantir l'interopérabilité d'un usager entre plusieurs domaines. Notre étude des travaux de R. Perlman dans [11], nous a permis nous orienter vers le modèle PKI en pont.

L'architecture PKI en pont permet, via l'utilisation de la certification croisée entre plusieurs CA (CA1 et CA2), de garantir l'opérabilité d'un certificat émis par un CA1 dans une PKI utilisant CA2.

Nous notons aussi que les autres besoins sécuritaires sont généralement remplis à travers la mise en place d'une PKI et outre mesure, la mise en place d'un chiffrement des messages transitant sur le réseau.

5.4 – Proposition d'une infrastructure PKI

L'implémentation PKI que nous proposons est basée sur l'architecture en pont et possède les spécificités suivantes :

- Implémentation d'un bridge CA (BCA)
- Création d'un certificat cosigné BCA/RootCA pour chaque domaine (interopérabilité entre les domaines)
- Limitation à deux CA intermédiaires par domaine (longueur du chemin de confiance limitée à 3)
- Utilisation de l'algorithme ECDSA (taille de certificat réduite)

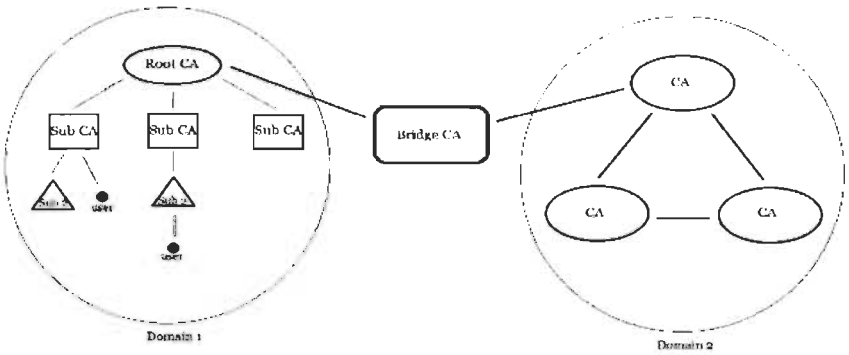

Figure 4: Schéma de notre proposition PKI

5.5 – Le simulateur OpenV2G

5.5.1 – Introduction

Afin de prouver l'apport des différentes améliorations que nous suggérons tout au long de ce travail, il était nécessaire de mettre en place plusieurs scénarios et d'étudier le comportement de notre système comparativement au système de base. Ainsi, la mise en place de ces scénarios dans le réseau V2G passe par l'utilisation d'un simulateur. Dans le cadre du V2G, il n'existe à l'heure actuelle qu'un seul simulateur permettant d'imiter le comportement des différents acteurs du réseau, il s'agit d'OpenV2G [**19**].

Le simulateur OpenV2G est issu de la collaboration de plusieurs organisations telles que l'institut des réseaux de communication de l'université de Dortmund (CNI) et de la compagnie Siemens. Ce programme est essentiellement basé sur le standard ISO15118 et il est distribué gratuitement sous forme de sources à compiler.

5.5.2 – Configuration du simulateur

Comme indiqué, OpenV2G est un logiciel basique fourni sous forme de sources dont le langage de programmation est le C. Ces fichiers sources sont exploitables à travers l'utilisation d'un environnement de développement (IDE), Éclipse étant l'IDE recommandé par les créateurs du projet.

Il n'existe à ce jour aucune documentation spécifique à OpenV2G, le simulateur étant toujours en cours de développement. Cependant, quelques exemples

de fonctionnement sont fournis à l'intérieur des fichiers sources afin de permettre une prise en main plus efficace en l'absence de documentation. Parmi ces exemples, on retrouve les cinématiques suivantes :

- « Handshake »

Prise de contact du véhicule électrique auprès de la borne de rechargement afin de spécifier les règles de communications des futurs échanges.

- « AC Charging »

Émission d'une demande de rechargement du PEV auprès de l'EVSE, en spécifiant que la nature du courant supporté est le courant alternatif.

- « DC Charging »

Émission d'une demande de rechargement du PEV auprès de l'EVSE, en spécifiant que la nature du courant supporté est le courant continu.

```
+++ Start application handshake protocol example +++

EV side: setup data for the supported application handshake request message
EV side: send message to the EVSE
EVSE side: List of application handshake protocols of the EV
        Protocol entry #=1
                ProtocolNamespace=urn:iso:15118:2:2010:MsgDef
                Version=1.0
                SchemaID=1
                Priority=1
        Protocol entry #=2
                ProtocolNamespace=urn:din:70121:2012:MsgDef
                Version=1.0
                SchemaID=2
                Priority=2
EV side: Response of the EVSE
                ResponseCode=OK_SuccessfulNegotiation
                SchemaID=1
+++ Terminate application handshake protocol example +++
```

Figure 5: Exemple de cinématique "Handshake" sans validation

5.5.3 – Changements apportés

Vu les limites inhérentes de l'utilisation du simulateur OpenV2G dans sa forme actuelle, il nous a donc été obligatoire de procéder à divers changements dans nos outils afin de mener à bien notre recherche.

Ces différents changements sont présentés en quatre points :

1. Logique orientée objet

Le langage C utilisé par le simulateur OpenV2G est un langage procédural. Afin de mettre en œuvre les différentes simulations nécessaires à notre travail de recherche, nous avons décidé d'adapter le code fourni dans les sources du simulateur dans un langage orienté objet, plus facilement modulable qui est le C#. Le code procédural utilisé étant très structuré et présentant beaucoup de similarités dans sa structure avec celle transposée au concept de l'oriente objet, la migration s'est donc faite sans accro.

2. Architecture Client / Serveur

Dans son état originel, OpenV2G ne prend en charge que la simulation d'un unique couple EVSE/PEV, limitant grandement les possibilités de mise en place de scénario d'attaques. Afin d'obtenir des données les plus proches du fonctionnement réel d'un réseau Vehicle-to-Grid, nous avons donc eu besoin d'implémenter une logique client/serveur nous permettant de mettre en relation plusieurs EV à un EVSE, ainsi que plusieurs EVSE dans un même réseau. Pour ce faire nous avons donc utilisé des sockets TCP/IP, les divers EVSE étant sur le même réseau chacun s'est vu attribuer un port diffèrent.

3. Bouncy Castle

Bouncy Castle est une Interface de Programmation applicative (API) qui se focalise sur la cryptographie, disponible en Java et en C#. Elle permet de mettre en œuvre une multitude de types de chiffrement que ce soit des algorithmes de chiffrement symétriques ou asymétriques. Dans nos travaux, nous avons eu à utiliser cette bibliothèque logicielle afin mettre en place des opérations de chiffrement basées sur les courbes elliptiques principalement, mais aussi afin de gérer les différentes opérations de gestion de certificats effectuées par notre simulateur.

Afin d'incorporer l'API Bouncy Castle [**20**] à notre projet, nous avons utilisé l'outil NuGet présent dans notre IDE, nous permettant d'importer la bibliothèque « BouncyCastle.Crypto.dll ».

Cette bibliothèque nous a alors permis de réaliser nos différentes opérations de chiffrement grâce aux classes suivantes :

- ECKeyPairGenerator : Permet de générer des clés de chiffrement ECDSA;
- RSAKeyPairGenerator : Permet de générer des clés de chiffrement RSA;
- KeyGenerationParameters : Permet de spécifier les paramètres de la clé à générer;
- SignerUtilities : Permet de générer et de vérifier une signature;
- SecNamedCurves : Permet de sélectionner la courbe elliptique à utiliser;
- FpFieldElement : Permet de spécifier les coordonnées x et y de la courbe;
- X509CertificatePair : Permet de générer une paire de certificats cosignés;

4. Base de données

Afin de gérer les différentes données véhiculaires et cryptographiques exploitées par notre simulateur nous avons eu à mettre en place une base de données. Cette base de données nous a permis d'exploiter plus efficacement les différentes données du simulateur tout en recueillant les différents résultats de nos simulations. Nous avons opté pour l'utilisation d'une base de données MySQL pour une mise en place simple. Nous avons donc eu à importer via l'outil NuGet la bibliothèque « MySQL.data ».

La figure 6 présente la base de données telle qu'elle a été conçue pour notre implémentation.

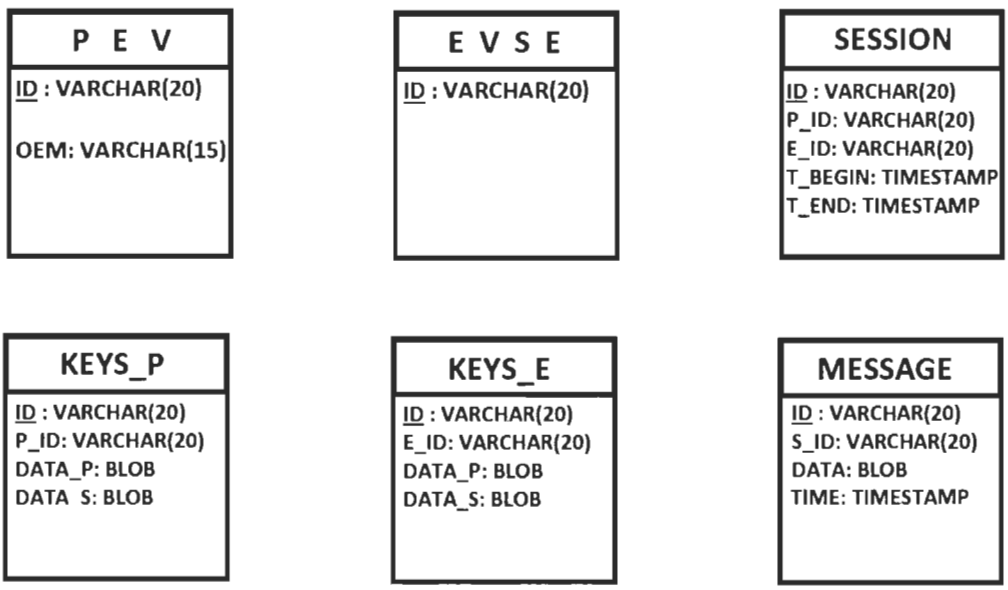

Figure 6: Représentation de la base de données

5.6 – Conclusion

Dans cette section nous avons présenté notre solution aux besoins sécuritaires du réseau V2G, en gardant pour objectif d'assurer la disponibilité, la confidentialité, l'authentification et l'anonymat. Ensuite, nous avons dévoilé les différents outils qui nous ont permis de mettre en place notre implémentation.

Dans le 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, ainsi que les métriques que nous avons utilisées afin de mettre en relief les performances de notre implémentation. Dans un second temps, nous allons présenter les différents résultats obtenus, ainsi que l'interprétation que nous en faisons.

Chapitre 6 – Simulations et Résultats

6.1 – Introduction

Les modifications apportées à notre simulateur nous permettent d'analyser le comportement du réseau V2G en fonction de différents scénarios d'attaque. Nous allons donc présenter l'environnement de test tel que nous l'avons mis en place pour notre travail de simulation ainsi que les différentes attaques simulées afin de pouvoir en analyser les résultats.

6.2 – Environnement de simulation

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 (PEV et EVSE). Dans un souci de reproduction des résultats, l'ordinateur utilisé possède les caractéristiques décrites dans le tableau 3.

Système d'exploitation	**Windows 10**
Nombre de cœurs physiques	4
Nombre de cœurs logiques	8
Fréquence du processeur	3,40 GHz
Mémoire vive	8 Go

Tableau 3: Caractéristiques de l'environnement de test

Durant les différents scénarios d'attaque, nous avons utilisé un échantillon de 20 PEV connectés à 5 EVSE pour une moyenne de 4 PEV par EVSE. Nous avons ainsi effectué 10 cinématiques d'échange complet par véhicule (initialisation de session, validation et clôture de session), afin d'écarter tout résultat aberrant, les simulations ont été répétées une dizaine de fois, à l'issue de laquelle les moyennes de ces résultats ont été calculées, les résultats seront présentés dans le paragraphe suivant. Le tableau 4 présente l'environnement du simulateur.

PARAMÈTRES	VALEURS
NOMBRES DE VÉHICULES	20
NOMBRES DE BORNES	5
NOMBRES DE MESSAGES PAR VÉHICULES	30
NOMBRES DE SIMULATIONS	10
DURÉE DE SIMULATION	1000 s

Tableau 4: Environnement du simulateur

6.3 – Les métriques de simulation

Les simulations que nous avons effectuées se sont principalement focalisées sur la performance du réseau en termes d'efficience de traitement des différents messages qui y transitent. Ainsi nous avons choisi d'utiliser trois métriques représentant au mieux les performances du réseau :

- Délai d'authentification (AD)

Le délai d'authentification correspond au temps nécessaire à un véhicule électrique d'être reconnu par une borne.

Un message « handshake » est donc envoyé par le PEV et il est reçu par l'EVSE qui à son tour renvoie un message contenant la réponse de la demande d'authentification.

Cette métrique nous permet de vérifier l'impact de notre implémentation sur la durée de traitement des messages dans le réseau.

- Délai d'envoi (SMD)

Le délai d'envoi correspond au temps nécessaire à un message, quel que soit son émetteur, d'être reçu par son destinataire.

En reprenant l'exemple du message « handshake », lorsque celui-ci est envoyé par le PEV à l'EVSE, le délai d'envoi correspond à la différence entre le temps de réception du message et le temps d'émission contenu dans le timestamp.

Cette métrique nous permet de vérifier l'impact de notre implémentation sur la rapidité des transmissions dans le réseau.

- Total de paquets perdus (TLP)

Le total de paquets perdus correspond au pourcentage de paquet qui ne sont pas arrivés jusqu'à leurs destinataires lors des différents échanges sur le réseau.

Lorsqu'un message « handshake » est envoyé par un PEV, et que ce message n'est pas reçu par l'EVSE auquel il est destiné, alors il est comptabilisé comme perdu. Le TLP est alors calculé en divisant le nombre de paquets perdus par le nombre de paquets envoyés.

Cette métrique nous permet de vérifier l'impact de notre implémentation sur la qualité des transmissions dans le réseau.

6.4 – Les attaques et les contremesures

Le réseau V2G a plusieurs besoins sécuritaires à combler. En outre, le réseau V2G doit être à même de pouvoir déjouer les diverses attaques dont il pourrait faire l'objet. Plusieurs types de scénarios d'attaques sont envisageables dans le « Vehicle-to-Grid ». Certaines attaques comme le « Denial-of-Service » (DOS) mettent en péril la stabilité du système, d'autres attaques comme le rejeu (ou « replay attack ») se focalisent sur la robustesse du réseau, enfin les attaques telles que celle de l'homme du milieu (ou « Man-in-the-Middle » ou MITM) en menacent l'imperméabilité.

Bien que le standard ISO 15118 adresse certains de ces besoins, force est de constater que certaines mises en œuvre ne sont pas des plus efficaces. C'est pourquoi certaines modifications sont nécessaires pour faire du V2G un réseau fiable et efficient.

Nous présentons ci-après les trois attaques (DOS, Rejeu, MITM), les solutions que nous avons proposées afin de bloquer ces attaques, et les performances du réseau.

6.4.1 – L'Homme du milieu

Dans un premier temps nous avons éprouvé notre implémentation avec une attaque de type MITM qui consiste en un individu interceptant un message lors d'une

communication entre deux entités pour prendre le contrôle de la communication. Il s'agit alors de falsifier la communication afin de se faire passer pour l'une des parties.

Dans le cadre du V2G nous l'avons adapté de telle sorte que lors de l'initialisation de la communication entre le PEV et l'EVSE, un attaquant puisse intercepter le message « handshake » afin de s'identifier auprès de la borne en tant que véhicule ciblé par l'attaque. Les communications entre deux entités du réseau V2G se font sur la base d'un identifiant de session ou « SessionID », cet identifiant reste le même durant toute la durée de la communication. En admettant qu'un attaquant puisse intercepter les messages échangés dans le réseau, il lui est alors possible d'usurper l'identité d'un des acteurs du réseau durant une conversation.

La proposition que nous soumettons afin de remédier à cette situation est d'établir un délai d'expiration de la session (T) au terme duquel un nouvel identifiant est généré. La figure 7 présente l'algorithme tel qu'utilisé.

```
ALGORITHME

Début
   Répéter pour chaque vèhicule
      Définir T;
      Nouvelle Session();
      Tant que (Session.date + T) > Système.date
         Engager communication;
      fin tant que;
      Clore Session;
   jusqu'à fin simulation;
Fin
```

Figure 7: Algorithme MITM

Malgré un trafic sur le réseau légèrement plus important à cause de la durée réduite des sessions, nous constatons à la figure 8 que la proportion de TLP reste similaire et les délais AD et MSD ne sont que peu impactés. Notre implémentation permet donc de déjouer l'attaque de l'homme du milieu, tout en sauvegardant les performances du réseau.

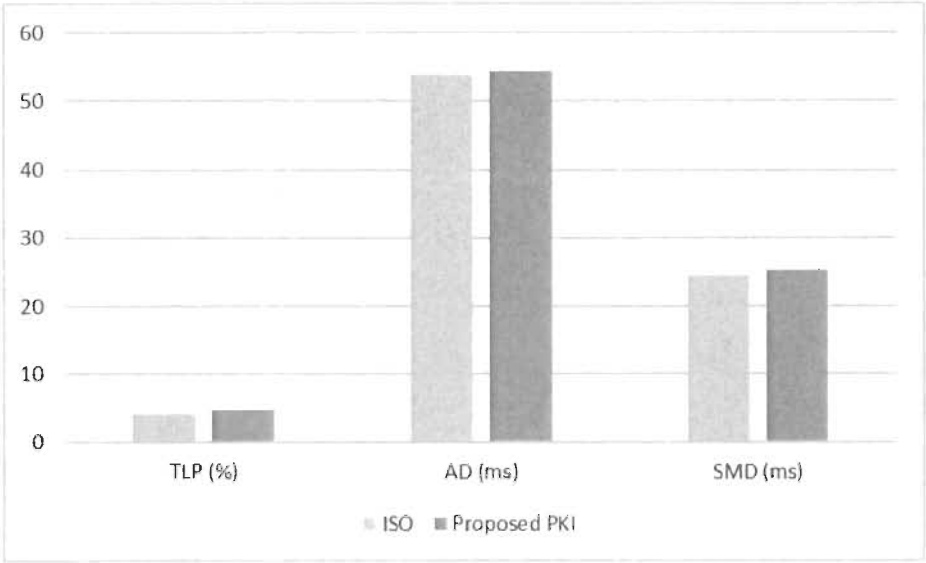

Figure 8: Résultats de la simulation du MITM

6.4.2 – Le Rejeu

Dans cette deuxième expérience, nous avons tenté de mettre en place une attaque de type rejeu dans laquelle un individu intercepte un message valide, comme celui d'authentification par exemple, pour le réutiliser lors de l'initiation d'une autre connexion avec le même destinataire afin d'usurper l'identité de l'émetteur original.

Les spécificités de l'ISO 15118 rendent la mise en place du rejeu difficile dans la mesure ou l'implémentation du « SessionID » devrait suffire en règle générale à contrer ce type d'attaque. Cependant, nous avons remarqué qu'au niveau de l'échange entre le PEV et l'EVSE pour l'établissement d'une session, le standard considère l'utilisation de l'horodatage comme optionnel. Ainsi dans ce cas précis, il serait judicieux de forcer le contrôle de l'horodatage afin de combler toute faille éventuelle. Comme on peut le constater à la figure 9, en forçant le contrôle de l'horodatage au niveau de la requête d'ouverture de session, le délai d'authentification (AD) est allongé, mais n'impacte ni le SMD ni le TLP. Notre implémentation permet donc de mettre à mal l'attaque de rejeu, tout en gardant un impact minime sur les performances, notamment sur celles du délai d'authentification.

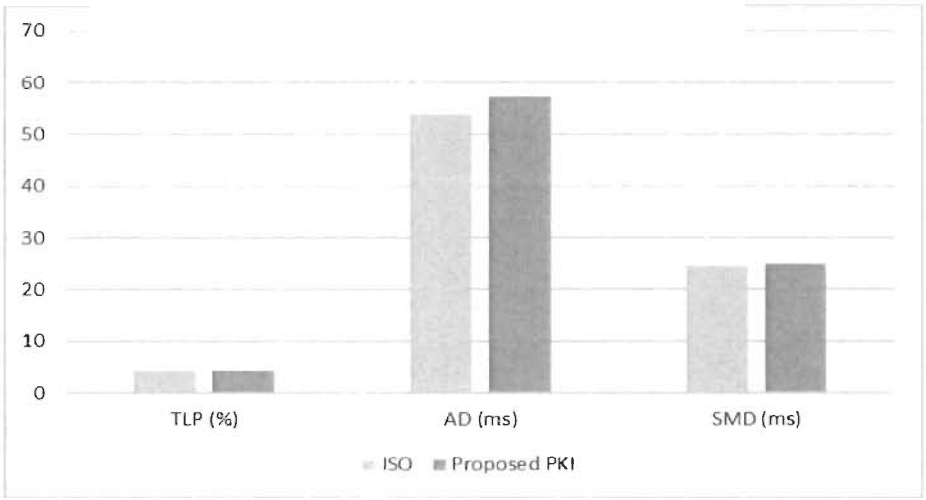

Figure 9: Résultats de la simulation du Rejeu

6.4.3 – Le Déni de service

Enfin, nous avons implémenté une attaque de déni de service (DOS) qui a pour principe l'envoi de messages en masse sur un réseau afin de rendre inutilisable une ressource, matérielle ou logicielle, auprès de ses utilisateurs. Ainsi, nous avons simulé cette attaque en essayant de noyer un EVSE sous un flot de fausses requêtes de rechargement afin de bloquer les demandes légitimes. Afin de lutter contre ce type d'attaque, nous avons proposé de mettre en place un système de détection. Pour cela, nous avons déterminé un seuil de requêtes **R** au-dessus duquel l'EVSE n'accepte plus de demandes émanant d'utilisateurs non précédemment authentifiés, pendant une période donnée (T). Pour nos simulations nous avons déterminé que **R** prendrait la valeur du nombre maximal de véhicules pouvant se connecter à la borne. La figure 10 présente l'algorithme tel qu'employé.

```
ALGORITHME

Début
   Répéter pour chaque borne
      Définir R, T, i, Start;
      Start = Système.date;
      i = 0
      Tant que Système.date < ( Start + T )
         Nouvelle Session();
         i = i + 1;
         Tant que i <> R
            Engager communication;
         fin tant que;
         Clore Session;
      fin tant que;
   jusqu'à fin simulation;
Fin
```

Figure 10: Algorithme DOS

Nous avons émis une hypothèse, similaire au « weak attack regime » évoqué dans [**8**], selon laquelle l'attaquant serait limité en ressources et ne pourrait donc profiter que d'un nombre limité d'accès sur le réseau. Ainsi, nous arrivons à limiter l'impact de l'attaque dans la mesure où la borne continue de fonctionner bien que son service soit restreint. Nous pouvons observer dans la figure 11 que le TLP est plus bas après la mise en place de la solution bien que le SMT et l'AD soient sensiblement les mêmes.

Ainsi, notre implémentation permet d'éviter la surcharge du réseau en cas de déni de service, tout en obtenant de meilleures performances.

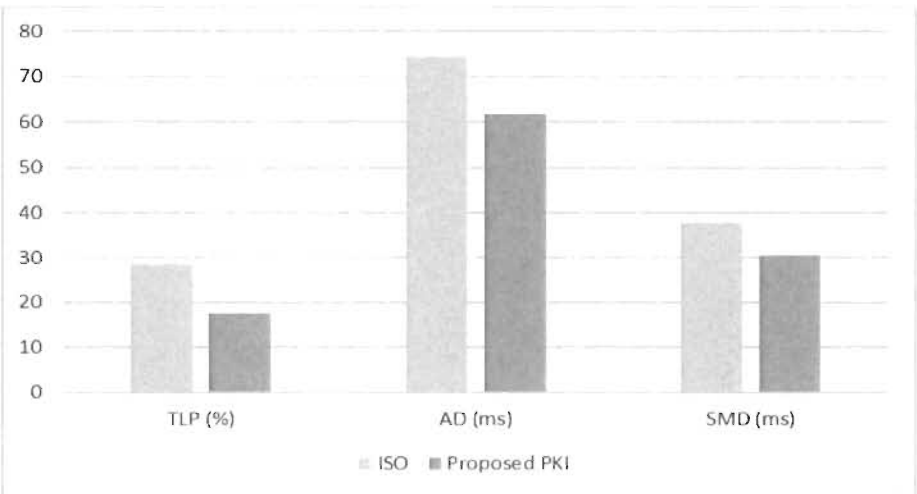

Figure 11: Résultats de la simulation DOS

6.4.4 – Analyse de sécurité

Notre solution impose la mise en place de la cryptographie à courbes elliptique pour les différents échanges du réseau. Ainsi les messages échangés sur le réseau, lorsqu'encryptés, ne peuvent être sujet à des attaques. Cependant, afin de prouver la sécurité assurée par notre proposition d'implémentation PKI, nous avons eu à éprouver notre solution face aux trois attaques présentées précédemment.

* Man-in-the-middle

Les échanges sur le réseau V2G sont chiffrés à l'aide des clés détenus par les différentes entités du réseau. De telle sorte que l'interception d'un message dans le but de s'immiscer dans un échange entre un véhicule et une borne, ne permettra pas à un attaquant d'exploiter la transmission interceptée, celui-ci ne disposant pas des clés nécessaires. En outre, notre implémentation permet grâce au changement régulier d'identifiant de session de renforcer la sécurité des échanges.

* Rejeu

L'attaque de rejeu consiste à capturer une transmission émise par un des acteurs du réseau V2G afin de réutiliser ce message plus tard. Cependant, notre implémentation rend obligatoire l'usage de l'horodatage. Ainsi, tous les messages échangés au sein de notre implémentation contiennent une trace du moment d'émission. En supposant qu'un attaquant réussisse à capturer un message, celui-ci ne pourra pas en modifier l'horodatage, ainsi l'entité visée par l'attaquant vérifiera l'horodatage et ignorera le message si celui-ci est ancien.

* Déni de Service

Malgré la mise en place du chiffrement des messages, l'attaque DOS est capable de perturber un réseau en l'inondant de transmissions indésirables et en accaparant les ressources à cause du traitement de ce flot de messages. Notre implémentation permet en cas d'attaque de type DOS, de détecter premièrement le nombre inhabituel de requêtes sur le réseau, et de limiter le traitement des messages indésirables en n'acceptant plus que les transmissions issues d'entités précédemment reconnu. Ainsi, lorsqu'une cinématique d'échange se déroule normalement, les entités participantes sont inscrites à une liste de confiance. Lorsque le seuil normal de messages dans le

réseau est atteint, seuls les messages dont les émetteurs se trouvent dans la liste de confiance seront traités.

6.5 – Étude comparative

Outre les différentes propositions d'améliorations de l'infrastructure sécuritaire que nous avons soumises, nous avons aussi été amenés à questionner le choix du standard ISO 15118 en termes de chiffrement.

6.5.1 – Les algorithmes de chiffrement

Afin de procéder à une authentification sécurisée entre les différents acteurs du réseau, le standard ISO préconise l'utilisation de l'algorithme de signature digital à courbe elliptique (ECDSA). Nous sommes donc à même de nous poser la question de l'avantage de l'utilisation des courbes elliptiques face à un algorithme plus répandu tel que le RSA.

Afin de procéder à cette comparaison, nous avons effectué les opérations suivantes :

- Génération de 25 certificats RSA et ECDSA pour des EV avec des niveaux de sécurité différents (256bits, 512bits, 1024bits) ;
- Initiation d'un message « handshake » pour les différents véhicules ;
- Mise en place d'un minuteur à la réception des messages au niveau de l'EVSE ;
- Traitement du message par l'EVSE ;
- Interruption de la minuterie à la génération de la réponse de l'EVSE.

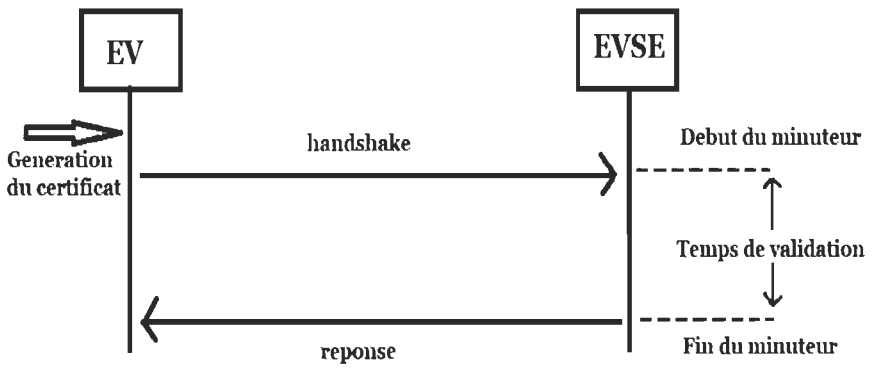

Figure 12: Illustration du temps de validation

Nous avons récupéré alors les différents temps mesurés et nous avons effectué une moyenne en fonction du chiffrement utilisé et du niveau de sécurité. Comme présenté dans la figure 12, le temps de validation correspond au délai entre la réception du « handshake » par l'EVSE et l'envoi de la réponse.

Pour ces simulations, nous avons effectué 250 opérations de chiffrement (10 par PEV) pour chaque algorithme pour chaque niveau de sécurité. Les simulations ont été répétées une dizaine de fois, à l'issue de quoi les moyennes sont présentées ci-après.

La figure 13 nous permet de constater que pour un même niveau de sécurité, le temps de validation du RSA est largement supérieur à celui de l'ECDSA et ce d'autant plus lorsque le niveau augmente.

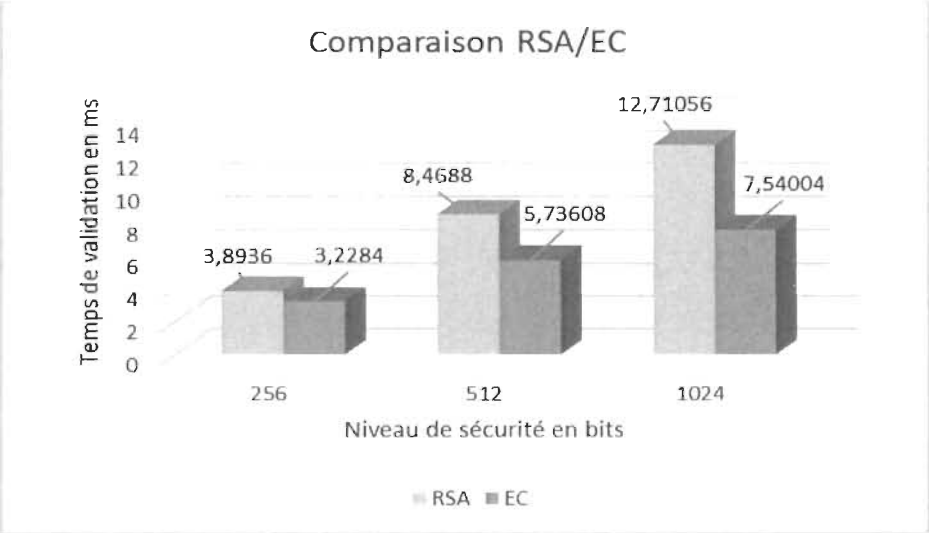

Figure 13: Comparaison des algorithmes RSA et ECDSA

L'utilisation des courbes elliptiques est donc sans aucun doute meilleure pour la sécurisation du réseau V2G afin d'obtenir un niveau de performance optimal.

6.5.2 – Les courbes elliptiques

Lors de la mise en place du chiffrement ECDSA, plusieurs choix de configuration sont proposés. En effet, plusieurs catégories de courbes elliptiques différentes peuvent être implémentées telles que X9.62, NIST, SEC et Teletrust avec différents niveaux de sécurité. Nous avons donc établi une comparaison des différentes courbes mise à notre disposition pour juger de l'impact en termes de performance. Les groupes X9.62, SEC, NIST et Teletrust sont respectivement représentés par les courbes c2pnb163v1, sect163k1, b-163 et brainpoolp160r1. Les opérations effectuées pour

obtenir nos résultats sont les mêmes que celles employées précédemment à la différence qu'ici nous n'avons employé qu'un seul niveau de sécurité pour les quatre courbes.

Pour ces simulations, nous avons effectué 250 opérations de chiffrement pour chaque courbe elliptique. Les simulations ont été répétées une dizaine de fois, à l'issue de laquelle les moyennes sont présentées ci-après.

Sur la figure 14, nous constatons que pour un niveau de sécurité égale, nous obtenons des performances quasi similaires, avec un léger avantage pour la courbe issue du groupe Teletrust.

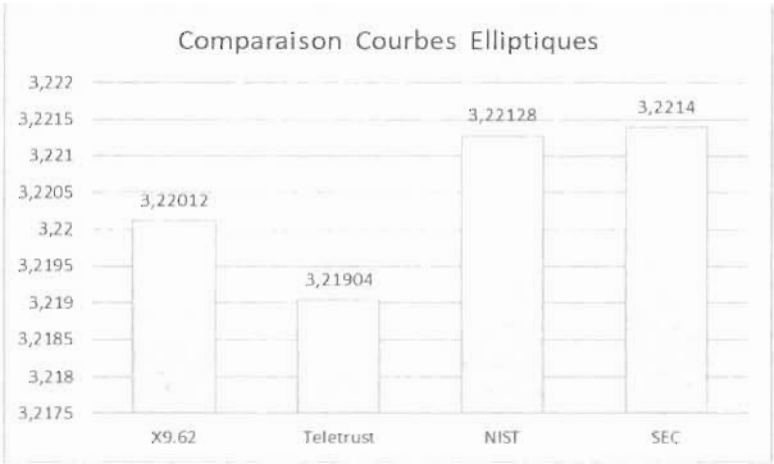

Figure 14: Comparaison des courbes elliptiques

6.6 – Conclusion

Dans cette partie, nous avons effectué l'évaluation de performances de nos diverses propositions afin de renforcer la sécurité des échanges du réseau V2G. Nous avons ainsi constaté qu'en général, nos contremesures aux attaques présentées précédemment permettent de renforcer la sécurité du réseau sans impact négatif sur le bon fonctionnement du réseau V2G. Dans nos travaux futurs, nous allons tenter d'améliorer nos propositions à travers des simulations plus poussées, permettant notamment de déterminer dans le cas de la contremesure au DOS une valeur optimale du seuil **R**.

Chapitre 7 – Conclusion générale et perspective

Dans le cadre de ce mémoire, nous avons analysé les travaux de références relatifs à la sécurité du réseau V2G en tentant de prendre en compte tous les aspects, soit du contexte de création jusqu'aux perspectives du réseau. La confiance qui sera accordée au réseau Vehicle-To-Grid reposera principalement sur sa capacité à protéger les informations confidentielles de ces divers utilisateurs ainsi qu'à assurer une disponibilité de ses services en toute circonstance. Nous notons ainsi que la mise en place d'une infrastructure à clés publiques est primordiale pour le bon fonctionnement du réseau. L'étude des différents travaux effectués dans le domaine ainsi que la prise en compte des spécifications existantes nous a permis de déterminer que l'architecture la plus adaptée est certainement l'architecture en pont. Suite à notre choix d'implémentation de PKI, nous avons eu à émettre plusieurs propositions permettant de limiter l'impact des attaques usuelles sur le réseau. L'objectif étant d'enrayer les conséquences néfastes de ces attaques tout en gardant un niveau de performances acceptable. Finalement, nous avons pu constater, à travers une étude comparative axée sur la partie cryptographie, que bien que des changements soient nécessaires au niveau du standard ISO, la solution de chiffrement proposée se montre optimale pour un réseau comme le V2G.

Les résultats de nos simulations sont assez concluants, dans la mesure où nos objectifs sécuritaires sont remplis, et les différents scenarios d'attaques sont bloqués par notre implémentation. Du point de vue des performances du réseau relevées à travers nos trois métriques, nous observons que dans le cas du « Man In The Middle » nos modifications n'affectent pas les performances du réseau, dans le cas du Rejeu seul le délai d'authentification est impacté et qu'au contraire, pour le Déni de Service, les performances sont améliorées.

Dans nos travaux futurs, nous avons l'intention d'approfondir l'étude de l'attaque DOS afin de déterminer un seuil R optimal en fonction des données du réseau (nombre de véhicules, nombre d'attaquants). Nous tenterons donc de nous rapprocher de cette valeur à travers une étude empirique.

Références bibliographiques

[1]Gharavi, H., & Ghafurian, R. (2011). Smart Grid: The Electric Energy System of the Future [Scanning the Issue]. Proceedings of the IEEE, 99(6), 917-921. doi:10.1109/JPROC.2011.2124210

[2]'https://www.bts.gov/archive/publications/pocket_guide_to_transportation/2017/7_Environment/table7_9_text' (accédé le 3 février 2017)

[3]'http://www.aveq.ca/actualiteacutes/statistiques-saaq-aveq-sur-lelectromobilite-au-quebec-en-date-du-31-decembre-2016-infographique' (accédé le 3 février 2017)

[4]'http://www.smartgridlibrary.com/2010/05/24/electric-vehicles-and-the-end-of-big-oil/' (accédé le 12 Aout 2016)

[5]'https://en.wikipedia.org/wiki/Efficient_XML_Interchange' (accédé le 12 Aout 2016)

[6]'ISO 15118-2: Road vehicles – Vehicle-to-Grid Communication Interface', ISO 2013

[7]Sorebo, G. N., & Echols, M. C. (2012). Smart grid security an end-to-end view of security in the new electrical grid. In (Vol. 27). Portland: Ringgold Inc.

[8]Kosut, O., Liyan Jia, R. J., Thomas, R. J., & Lang Tong, R. J. (2011). Malicious Data Attacks on the Smart Grid. Smart Grid, IEEE Transactions on, 2(4), 645-658. doi:10.1109/TSG.2011.2163807

[9]Liu, Y., Ning, P., & Reiter, M. (2011). False data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security (TISSEC), 14(1), 1-33. doi:10.1145/1952982.1952995

[10]Tim Moses (2012). PKI Trust Models. IETF

[11]Perlman, R. (1999). An overview of PKI trust models. Network, IEEE, 13(6), 38-43. doi:10.1109/65.806987

[12]He, D., Chan, S., Zhang, Y., Guizani, M., Chen, C., & Bu, J. (2014). An enhanced public key infrastructure to secure smart grid wireless communication networks. IEEE Network, 28(1), 10-16. doi:10.1109/MNET.2014.6724101

[13]Baumeister, T. (2011). Adapting PKI for the smart grid. In (pp. 249-254).

[14]Mingchu, L., Yizhi, R., Zhihui, W., Jun, X., & Hongyan, Y. (2006). A New Modified Bridge Certification Authority PKI Trust Model. In (pp. 23-26).

[15]Han, W., & Xiao, Y. (2016). Privacy preservation for V2G networks in smart grid: A survey. Computer Communications, 91-92, 17-28. doi:10.1016/j.comcom.2016.06.006

[16]Saxena, N., Choi, B. J., & Cho, S. (2015, 20-22 Aug. 2015). Lightweight Privacy-Preserving Authentication Scheme for V2G Networks in the Smart Grid. Paper presented at the 2015 IEEE Trustcom/BigDataSE/ISPA.

[17]Liping, Z., Shanyu, T., & He, L. (2016). Elliptic Curve Cryptography-Based Authentication with Identity Protection for Smart Grids. PLoS ONE, 11(3), e0151253. doi:10.1371/journal.pone.0151253

[18]Vaidya, B., Makrakis, D., & Mouftah, H. (2014). Effective public key infrastructure for vehicle-to-grid network. Paper presented at the Proceedings of the fourth ACM international symposium on Development and analysis of intelligent vehicular networks and applications, Montreal, QC, Canada.

[19]'http://openv2g.sourceforge.net/' (accédé le 10 janvier 2015)

[20]'http://www.bouncycastle.org/csharp/' (accédé le 9 juin 2015)