Chapitre 1

Introduction

Dans cette partie, nous allons tout d'abord présenter la start-up One Wave ainsi que son projet de carte universelle connectée, sur lequel nous avons travaillé. Nous ferons ensuite une rapide introduction à la Tokenisation qui a été le fil conducteur de notre travail. Nous finirons par présenter le planning final, que nous avons suivi tout au long du projet.

1.1 One Wave

One Wave est une jeune start-up basée à Rennes, fondée en juin 2016. C'est un projet qui a été initié par Thomas Lechevallier et qui compte aujourd'hui huit personnes dont sept sont fondateurs de l'entreprise.

FIGURE 1.1 – One Wave : logo de l'entreprise.

L'objectif des membres de One Wave est de créer une carte universelle connectée, que nous allons présenter dans la section suivante.

1.2 Le projet One Wave : Une carte universelle connectée

Ce projet de carte universelle connectée vise à regrouper toutes les cartes d'un utilisateur en une seule. Cela ne concerne pas uniquement les cartes bancaires qu'elles soient personnelles ou professionnelles, mais aussi les cartes de fidélité ainsi que les cartes et les tickets de transport.
Cette carte doit pouvoir être configurée à distance grâce à une application mobile, pour permettre l'ajout et la suppression de cartes, la configuration de la sécurité et l'accès à des informations contextuelles.

FIGURE 1.2 – Concept de la carte universelle connectée.

Le travail qui nous a été demandé concernait surtout l'aspect bancaire, et plus particulièrement le transport d'informations contextuelles au sein d'une transaction EMV. C'est pourquoi la première partie de notre travail a consisté à étudier la spécification EMV "Payment Tokenisation Specification", de manière à nous familiariser avec la Tokenisation.

1.3 Introduction à la Tokenisation

1.3.1 Définition d'un Token

Dans le cadre d'une transaction, un Token est une donnée "jetable", aussi appelée jeton de paiement, permettant de remplacer les données bancaires telles que le PAN (Personal Account Number).
Ainsi, le processus de Tokenisation consiste à générer un Token à partir du PAN et de sa date d'expiration [Figure 1.3].

FIGURE 1.3 – Principe de la Tokenisation.

Inversement, le processus de Detokenisation permet de récupérer le PAN et sa date d'expiration à partir du Token [Figure 1.4].

FIGURE 1.4 – Principe de la Detokenisation.

1.3.2 Pourquoi les Token ?

Dans le cadre des transactions EMV :

L'utilité des Tokens réside dans le fait qu'ils permettent d'assurer l'intégrité et la confidentialité du PAN lors d'une transaction EMV. En effet, en cas d'interception, le PAN a peu de chance d'être récupéré ce qui limite les risques. Cela permet aux banques émetteurs de réduire la fraude et aux commerçants de ne pas avoir à stocker les informations clients dans leur système d'information.

De ce fait, les Tokens sont notamment utilisés lors des paiements NFC (Near Field Communication), lors de l'utilisation d'une wallet (i.e. Apple Pay) ou dans le domaine du e-Commerce.

Dans le cadre du projet :

En plus d'être un élément de sécurité, l'utilisation des Tokens nous permet de transporter de l'information supplémentaire lors des transactions.

1.4 Planning

Du 05/10 au 02/11	Etude la spécification EMVCo
09/11	Présentation blanche à Rennes de la soutenance de mi-parcours
16/11	Soutenance de mi-parcours
Du 16/11 au 23/11	Etude des champs de données libres + Mise en place des outils de travail + Ecriture du rapport (1ère partie)
Du 23/11 au 30/11	Fin écriture du rapport (1ère partie)
Du 30/11 au 18/01	Partie développement : Implémentation d'un Token Service Provider (Tokenisation / Detokenisation)
Du 18/01 au 25/01	Recette + Ecriture du rapport (2ème partie)
25/01	Présentation blanche de la soutenance finale
01/02	Soutenance finale

FIGURE 1.5 – Planning final du projet.

Chapitre 2

Etude de la spécification EMVCo "Payment Tokenisation Specification", 2014

Dans ce chapitre, nous allons revenir sur notre étude de la spécification pour détailler les différentes phases d'une transaction avec Token de façon claire. Dans un premier temps, nous introduirons deux nouveaux acteurs qui n'interviennent pas dans une transaction EMV classique, mais seulement dans une transaction avec Token. Ensuite, nous présenterons les différents éléments de données avant de nous intéresser de plus près à une transaction EMV avec Token, à travers quatre cas d'usage bien précis.

Ci-dessous se trouve le schéma global d'une transaction EMV avec Token [Figure 2.1]. Dans les parties 2.3, 2.4 et 2.5, nous allons découper ce schéma pour le détailler plus amplement.

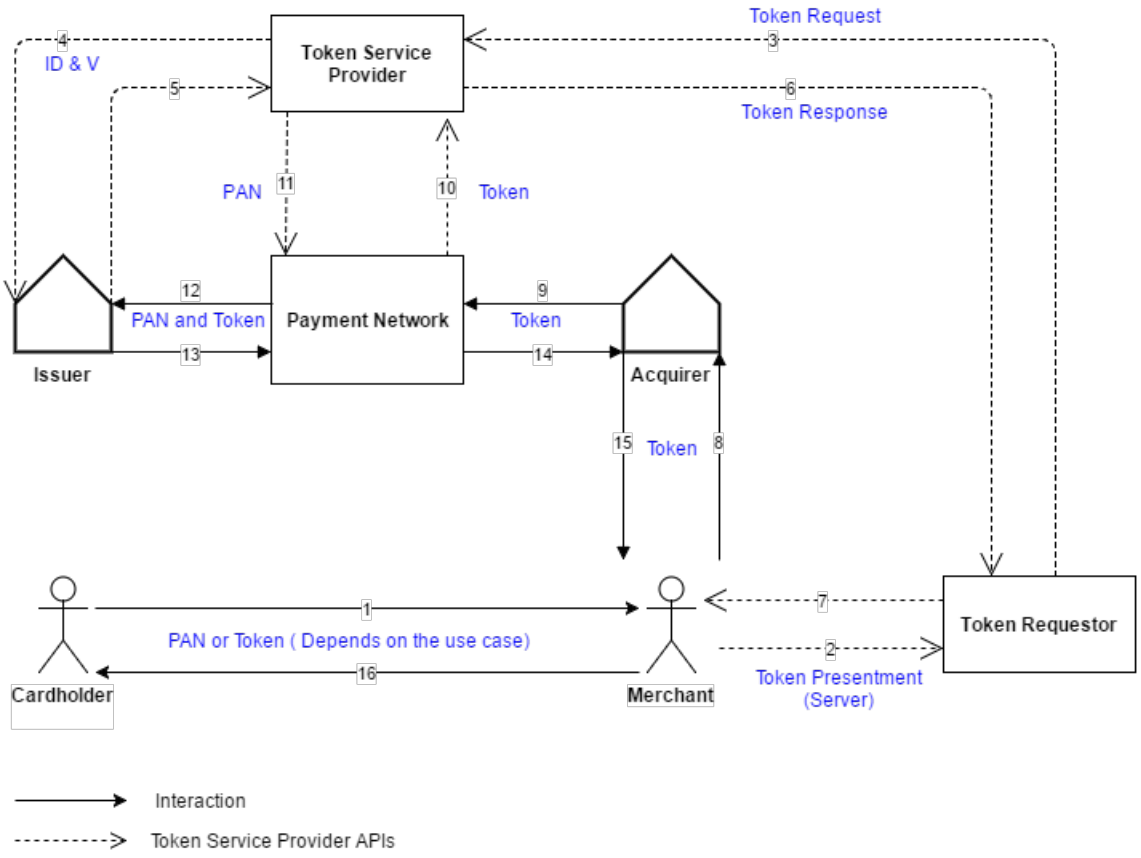

FIGURE 2.1 – Schéma global d'une transaction EMV avec Token.

2.1 Token Service Provider et Token Requestor

2.1.1 Token Service Provider

Le Token Service Provider a pour rôle de fournir les Tokens et de gérer leur cycle de vie. Pour cela, il se doit également d'implémenter toutes les interfaces liées aux services du Token et de garantir la sécurité du Token ainsi que l'association PAN / Token.
Lors d'une transaction, le Token Service Provider peut être n'importe quel acteur, c'est-à-dire, la banque émetteur, la banque acquéreur, le commerçant, le réseau de paiement ou encore une tierce partie.

2.1.2 Token Requestor

Le Token Requestor est, quant à lui, responsable des demandes de génération de Token et de changement d'état du Token, notamment en cas de perte ou de vol de celui-ci. Toutefois, avant de pouvoir faire une demande de génération de Token, le Token Requestor doit impérativement s'être au préalable enregistré auprès d'un ou plusieurs Token Service Provider.
Lors d'une transaction, le token Requestor peut être la banque émetteur, la banque acquéreur, le commerçant ou bien une tierce partie comme par exemple un gestionnaire de wallet. Cependant, contrairement au Token Service Provider, le Token Requestor ne sera en aucun cas le réseau de paiement.

2.2 Les Data elements

2.3 Demande et émission de Token

Lors d'une transaction EMV, lorsque le PAN n'est pas déjà lié à un Token valide et qu'un Token est requis, le Token Requestor envoie une demande de génération de Token au Token Service Provider. Cette requête contient donc le PAN et sa date d'expiration, ainsi que le Token Requestor ID. Ensuite, le Token service Provider va se charger d'envoyer une demande d'identification et vérification à la banque émetteur, pour déterminer le Token Assurance Level et le Token Assurance Data. Une fois cette étape validée, le Token Service Provider génère le Token qu'il transmet au Token Requestor, en plus de la date d'expiration du Token, du Token Assurance Level et du Token Assurance Data.

Le schéma suivant résume la demande et l'émission d'un Token [Figure 2.2].

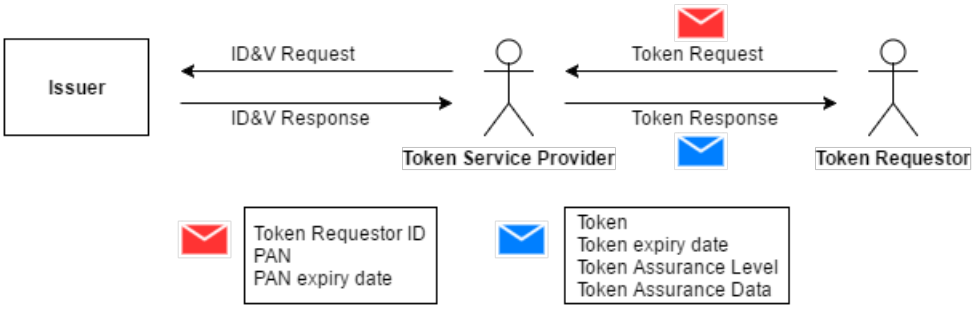

FIGURE 2.2 – Demande et émission d'un Token.

Dans les deux sous-parties qui suivent, nous présenterons davantage les méthodes d'identification et vérification, et les interfaces qui doivent être implémentées par le Token Service Provider.

2.3.1 Les méthodes d'Identification et Vérification

2.3.2 Les interfaces : Token Service Provider APIs

2.4 Transaction EMV avec Token

Dans cette section, nous allons d'abord présenter l'interaction client-commerçant de manière à introduire les différents cas d'usage, impliquant un Token, utilisés dans la spécification. Dans un second temps, nous verrons comment se poursuit la transaction avec le Token, depuis le commerçant vers les autres acteurs de la transaction.

2.4.1 Côté client - commerçant

Dans la spécification, l'interaction client - commerçant, lors d'une transaction EMV avec Token, est présentée à travers les paiements NFC mobile, par QR code, par wallet et via les sites de e-Commerce.

Ce dernier cas est d'ailleurs un peu particulier puisque, lorsque le client fait des achats sur le site d'un commerçant pour la première fois, celui-ci va lui demander de lui envoyer le PAN [Figure 2.3]. En général, le client doit remplir un formulaire avec les données inscrites sur sa carte. Le PAN ne sera pas stocké par le commerçant mais celui-ci va directement contacter le Token Requestor pour qu'il fasse une demande de génération de Token. Par la suite, c'est le Token qui sera stocké par le commerçant. C'est ce qu'on appelle le Card-on-File. Ainsi, le client est en quelque sorte enregistré auprès du commerçant, et lorsqu'il fera d'autres achats sur ce site, le commerçant utilisera le Token lié au PAN du client, qu'il aura conservé dans un fichier. Ici, c'est donc côté commerçant qu'est stocké le Token.

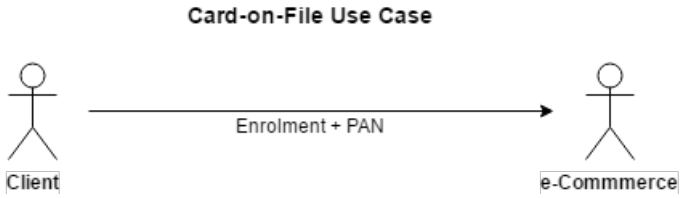

FIGURE 2.3 – Interaction client-commerçant pour le cas d'usage Card-on-file.

Pour les trois autres cas d'usage, le Token est conservé côté client, c'est-à-dire, stocké dans l'appareil du client, qui est son téléphone mobile dans la plupart des cas. En effet, lors d'une transaction, c'est le client qui envoie au commerçant le Token, sa date d'expiration, le Token cryptogram et éventuellement le Token Requestor ID [Figure 2.4].
A noter également que, dans le cas du QR code, le client transmet aussi les données du QR code au commerçant. Dans le cas du NFC mobile, il peut y avoir des échanges de données avec un cloud au préalable.

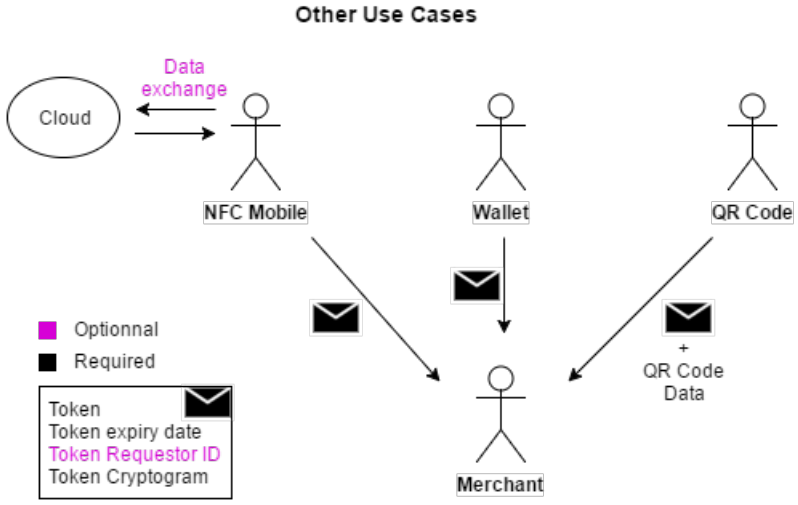

FIGURE 2.4 – Interaction client-commerçant pour les cas d'usage : NFC mobile, Wallet, QR Code.

2.4.2 Côté commerçant - autres acteurs de la transaction

Une fois la transaction engagée entre le client et le commerçant, ce dernier envoie une demande d'autorisation à sa banque acquéreur et lui transmet les données que le client lui a envoyé ainsi que le Point Of Sell Entry Mode ou mode d'acceptation [Figure 2.5]. Dans le cas du e-Commerce, l'identifiant du commerçant est également transmis à la banque acquéreur.
Ensuite, celle-ci va rediriger toutes ces données vers le réseau de paiement, qui va alors contacter le Token Service Provider pour que celui-ci fasse l'association entre le Token et le PAN correspondant. Le Token Service Provider renvoie donc le PAN au réseau de paiement, mais aussi le Token Assurance Data et le Token

Assurance Level. C'est la phase de detokenisation. Ainsi, le réseau de paiement va envoyer les données qu'il a reçu de la banque acquéreur et du Token Service Provider à la banque émetteur, c'est-à-dire, le couple PAN/Token et les données correspondantes. La banque émetteur reçoit donc la demande d'autorisation et peut ou non la valider.
Enfin, le résultat de la demande d'autorisation et le PAN sont retransmis au réseau de paiement qui va remplacer le PAN par le Token correspondant, avant de faire recirculer ces données vers la banque acquéreur, qui va les transmettre au commerçant.

Le schéma ci-dessous résume le déroulement d'une transaction EMV avec Token, à partir du commerçant.

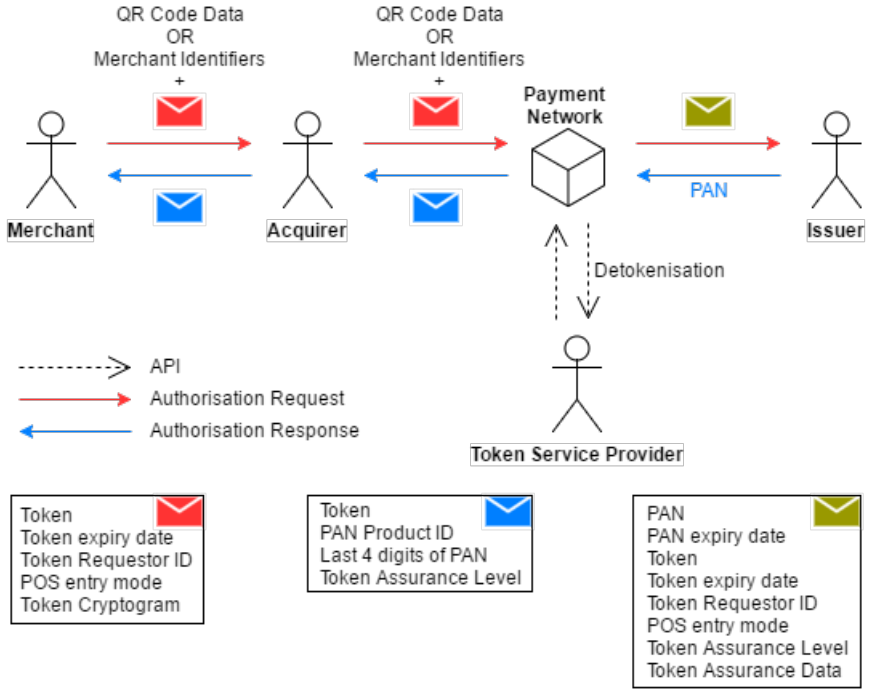

FIGURE 2.5 – Interaction commerçant-autres acteurs de la transaction.

2.5 Acquisition, compensation, règlement

Dans cette partie, nous allons présenter les processus d'acquisition, de compensation et de règlement, qui se déroulent pendant et après la télécollecte.

Dans le cadre du projet, nous ne nous intéresserons pas à ces trois phases, mais il est nécessaire de les détailler ici puisqu'elles sont présentées dans la spécification.

2.5.1 Acquisition et compensation

Lors de la phase d'acquisition/compensation, le commerçant envoie d'abord un fichier d'acquisition à sa banque acquéreur. Ce fichier contient le Token, sa date d'expiration, le Token Assurance Level et éventuellement le Token Requestor ID. Ensuite, la banque acquéreur vérifie les éléments de données contenus dans ce fichier et y ajoute le mode d'acceptation pour constituer un fichier de compensation qu'elle va envoyer au réseau de paiement. Tout comme pour la transaction, celui-ci va demander au Token Service Provider de faire le mapping entre le Token et le PAN pour pouvoir ensuite transmettre le fichier de compensation complété à la banque émetteur, qui devra valider ou non la compensation et renvoyer sa réponse au réseau de paiement.

Le schéma ci-dessous détaille les champs de données qui transitent lors des phases d'acquisition puis de compensation [Figure 2.6].

2.5.2 Règlement

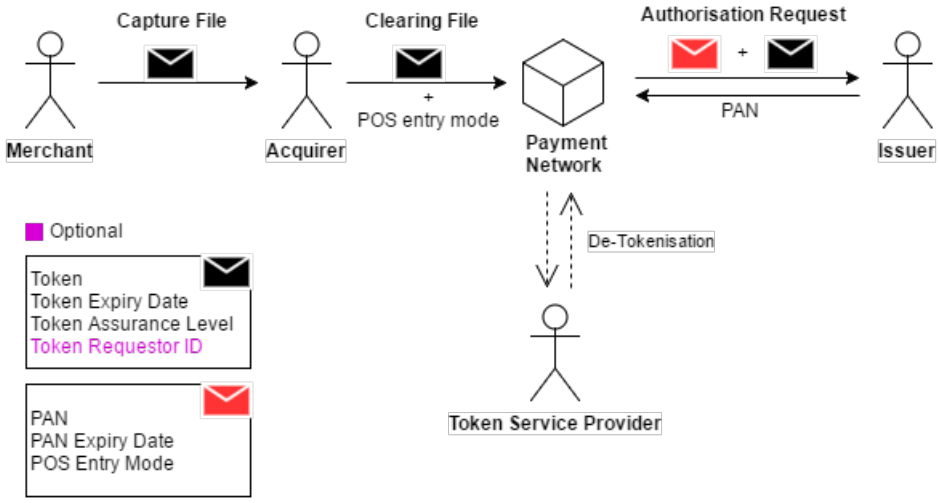

FIGURE 2.6 – Acquisition et compensation.

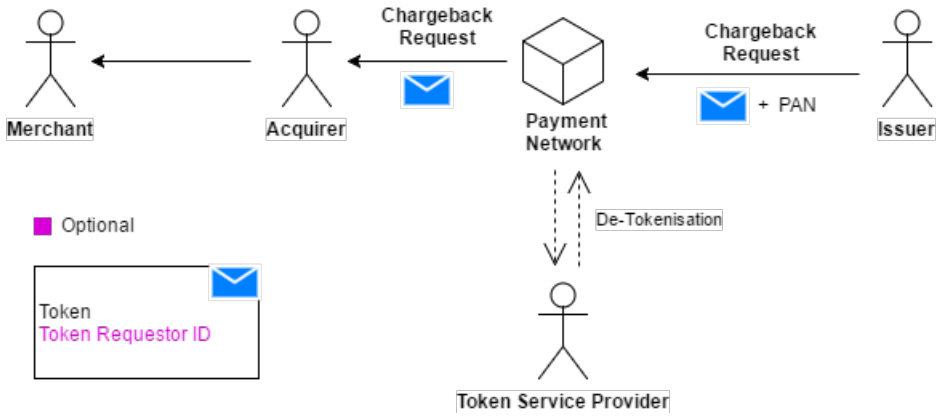

FIGURE 2.7 – Règlement.